The Polycom RealPresence DMA System is also known and certified as the DMA System.
Copyright© 2017, Polycom, Inc. All rights reserved. No part of this document may be reproduced, translated into another language or format, or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Polycom, Inc.

6001 America Center Drive
San Jose, CA 95002
USA

**Trademarks** Polycom®, the Polycom logo and the names and marks associated with Polycom products are trademarks and/or service marks of Polycom, Inc., and are registered and/or common law marks in the United States and various other countries.

All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Polycom.

**Disclaimer** While Polycom uses reasonable efforts to include accurate and up-to-date information in this document, Polycom makes no warranties or representations as to its accuracy. Polycom assumes no liability or responsibility for any typographical or other errors or omissions in the content of this document.

**Limitation of Liability** Polycom and/or its respective suppliers make no representations about the suitability of the information contained in this document for any purpose. Information is provided "as is" without warranty of any kind and is subject to change without notice. The entire risk arising out of its use remains with the recipient. In no event shall Polycom and/or its respective suppliers be liable for any direct, consequential, incidental, special, punitive or other damages whatsoever (including without limitation, damages for loss of business profits, business interruption, or loss of business information), even if Polycom has been advised of the possibility of such damages.

**End User License Agreement** BY USING THIS PRODUCT, YOU ARE AGREEING TO THE TERMS OF THE END USER LICENSE AGREEMENT (EULA) AT: http://documents.polycom.com/indexes/licenses. IF YOU DO NOT AGREE TO THE TERMS OF THE EULA, DO NOT USE THE PRODUCT, AND YOU MAY RETURN IT IN THE ORIGINAL PACKAGING TO THE SELLER FROM WHOM YOU PURCHASED THE PRODUCT.

**Patent Information** The accompanying product may be protected by one or more U.S. and foreign patents and/or pending patent applications held by Polycom, Inc.

**Open Source Software Used in this Product** This product may contain open source software. You may receive the open source software from Polycom up to three (3) years after the distribution date of the applicable product or software at a charge not greater than the cost to Polycom of shipping or distributing the software to you. To receive software information, as well as the open source software code used in this product, contact Polycom by email at OpenSourceVideo@polycom.com.

**Customer Feedback** We are striving to improve our documentation quality and we appreciate your feedback. Email your opinions and comments to DocumentationFeedback@polycom.com.

**Polycom Support** Visit the Polycom Support Center for End User License Agreements, software downloads, product documents, product licenses, troubleshooting tips, service requests, and more.
## Contents

### Getting Started ................................................. 23

**Polycom® RealPresence® DMA® System Overview ................... 24**
- The Polycom RealPresence DMA System’s Primary Functions ........... 24
- Conference Manager ........................................... 24
- Call Server .................................................... 25
- RealPresence® Platform API .................................... 25
- SVC Conferencing Support ..................................... 26
- The Polycom RealPresence DMA System’s Three Configurations .......... 27
  - Two-server Configuration .................................... 27
  - Single-server Configuration ................................ 28
  - Supercluster Configuration .................................. 28
  - Clusters versus Superclusters ................................. 28
- Polycom Solution Support ....................................... 29

### Working in the Polycom® RealPresence® DMA® System ............... 30
- Log In to the System .......................................... 30
- Sign Out of the System ........................................ 30
- Change Your Password ........................................ 31
- Dashboard ....................................................... 31
  - Dashboard Panes ............................................... 31
    - Active Directory Integration Pane .......................... 31
    - Call Server Active Calls Pane ............................. 32
    - Call Server Registrations Pane ............................ 32
    - Cluster Info Pane ........................................... 32
    - Conference History – Max Participants Pane .............. 32
    - Conference Manager MCUs Pane ........................... 33
    - Conference Manager Usage Pane .......................... 33
    - Exchange Server Integration Pane ........................ 33
    - High Availability Status Pane .............................. 34
    - RealPresence Resource Manager System Integration Pane .................. 34
    - Server Interfaces Pane .................................... 34
    - Signaling Settings Pane ................................... 35
    - Supercluster Status Pane ................................ 35
## Initial System Configuration

- DNS Records for the Polycom RealPresence DMA System ........................................ 41
  - Add Required DNS Records for the Polycom RealPresence DMA System .................. 42
  - Add DNS Records for SIP Proxy  ........................................................................ 42
  - Add DNS Records for the H.323 Gatekeeper ...................................................... 43
  - Add DNS Records for the Embedded DNS Server .............................................. 43
  - Verify That DNS Is Working for All Addresses .................................................. 44
- License the Polycom RealPresence DMA System .................................................... 44
- Set Up Signaling ..................................................................................................... 44
- Configure the Call Server and Optionally Create a Supercluster ............................. 45
- Set Up Security ....................................................................................................... 45
- Set Up MCUs .......................................................................................................... 46
- Connect to Microsoft Active Directory® ............................................................... 47
- Set Up Conference Templates ................................................................................ 48
- Test the System ........................................................................................................ 49

## Server Configuration

### Server Settings

- Network Settings ..................................................................................................... 51
  - Configure General System Network Settings ...................................................... 51
  - Configure Network Interface Settings .................................................................. 53
  - Configure Service Settings .................................................................................. 54
  - Routing Configuration ........................................................................................... 55
    - Add a Static Route ............................................................................................... 55
    - Delete a Static Route ........................................................................................... 56
  - Bonded and VLAN Interfaces ................................................................................. 56
    - Add a Bonded Interface ....................................................................................... 56
    - Edit a Bonded Interface ...................................................................................... 59
### Contents

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a VLAN Interface</td>
<td>61</td>
</tr>
<tr>
<td>Edit a VLAN Interface</td>
<td>62</td>
</tr>
<tr>
<td>Enable IPv6</td>
<td>63</td>
</tr>
<tr>
<td>Enable IPv4</td>
<td>63</td>
</tr>
<tr>
<td>Configure Time Settings</td>
<td>63</td>
</tr>
<tr>
<td>Configure Logging Settings</td>
<td>64</td>
</tr>
<tr>
<td>Configure Alert Settings</td>
<td>65</td>
</tr>
<tr>
<td>Changing the Linux Root Password</td>
<td>66</td>
</tr>
<tr>
<td>Change the Linux Root Password</td>
<td>67</td>
</tr>
<tr>
<td>Usage Data</td>
<td>67</td>
</tr>
<tr>
<td>Enable or Disable Automatic Data Collection</td>
<td>68</td>
</tr>
<tr>
<td>See the Collected Usage Data</td>
<td>68</td>
</tr>
<tr>
<td><strong>Signaling Settings</strong></td>
<td>70</td>
</tr>
<tr>
<td>H.323, SIP, and WebRTC Signaling</td>
<td>70</td>
</tr>
<tr>
<td>The RealPresence DMA System as a SIP &lt;-&gt; H.323 Gateway</td>
<td>70</td>
</tr>
<tr>
<td>Configure SIP Settings</td>
<td>70</td>
</tr>
<tr>
<td>Configure H.323 Settings</td>
<td>71</td>
</tr>
<tr>
<td>Configure WebRTC Settings</td>
<td>72</td>
</tr>
<tr>
<td>Untrusted SIP Call Handling</td>
<td>72</td>
</tr>
<tr>
<td>Guest Ports</td>
<td>73</td>
</tr>
<tr>
<td>Add a New Guest Port</td>
<td>73</td>
</tr>
<tr>
<td>Edit a Guest Port</td>
<td>73</td>
</tr>
<tr>
<td>Dial Rules for Guest Calls</td>
<td>74</td>
</tr>
<tr>
<td>Add a Dial Rule for Guest Calls</td>
<td>74</td>
</tr>
<tr>
<td>Edit a Dial Rule for Guest Calls</td>
<td>75</td>
</tr>
<tr>
<td><strong>High Availability Settings</strong></td>
<td>76</td>
</tr>
<tr>
<td>Network Settings to Support High Availability</td>
<td>76</td>
</tr>
<tr>
<td>High Availability Requirements</td>
<td>77</td>
</tr>
<tr>
<td>Configure High Availability Settings</td>
<td>77</td>
</tr>
<tr>
<td>Change High Availability Password</td>
<td>79</td>
</tr>
<tr>
<td>High Availability Licensing</td>
<td>80</td>
</tr>
<tr>
<td>Certificates for High Availability Systems</td>
<td>80</td>
</tr>
<tr>
<td>Requesting Signed Certificates</td>
<td>81</td>
</tr>
<tr>
<td>Integrating High Availability Systems with the RealPresence Resource Manager System</td>
<td>81</td>
</tr>
<tr>
<td>DNS Records for High Availability</td>
<td>81</td>
</tr>
<tr>
<td><strong>Licenses</strong></td>
<td>82</td>
</tr>
<tr>
<td>View License Information</td>
<td>82</td>
</tr>
<tr>
<td>Contents</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Adding Licenses</td>
<td>83</td>
</tr>
<tr>
<td>Adding a License to the RealPresence DMA System, Appliance Edition</td>
<td>83</td>
</tr>
<tr>
<td>Request a Software Activation Key Code for the Server</td>
<td>84</td>
</tr>
<tr>
<td>Enter a License Activation Key Code</td>
<td>84</td>
</tr>
<tr>
<td>Adding a License to the RealPresence DMA System Using the RealPresence Resource Manager System</td>
<td>85</td>
</tr>
<tr>
<td>Security Settings</td>
<td>86</td>
</tr>
<tr>
<td>Selecting a Security Mode</td>
<td>86</td>
</tr>
<tr>
<td>Configure Security Settings</td>
<td>86</td>
</tr>
<tr>
<td>Restrict Security Ciphers</td>
<td>90</td>
</tr>
<tr>
<td>Security Certificates</td>
<td>92</td>
</tr>
<tr>
<td>How Certificates Are Used</td>
<td>92</td>
</tr>
<tr>
<td>Accepted Certificates</td>
<td>93</td>
</tr>
<tr>
<td>Certificate Signing Requests</td>
<td>94</td>
</tr>
<tr>
<td>Certificate Signing Request Requirements</td>
<td>94</td>
</tr>
<tr>
<td>Create a Certificate Signing Request</td>
<td>95</td>
</tr>
<tr>
<td>View an Encoded Certificate Signing Request</td>
<td>97</td>
</tr>
<tr>
<td>Add a Subject Alternative Name (SAN) Extension</td>
<td>97</td>
</tr>
<tr>
<td>Edit a Subject Alternative Name (SAN) Extension</td>
<td>97</td>
</tr>
<tr>
<td>Installing Certificates</td>
<td>98</td>
</tr>
<tr>
<td>View Installed Certificates</td>
<td>99</td>
</tr>
<tr>
<td>Display Certificate Details</td>
<td>100</td>
</tr>
<tr>
<td>Install a Certificate Authority’s Certificate</td>
<td>100</td>
</tr>
<tr>
<td>Install a Signed Certificate</td>
<td>101</td>
</tr>
<tr>
<td>Removing Certificates</td>
<td>102</td>
</tr>
<tr>
<td>Remove a Trusted Root CA’s Certificate</td>
<td>102</td>
</tr>
<tr>
<td>Remove a Signed Certificate</td>
<td>103</td>
</tr>
<tr>
<td>History Retention Settings</td>
<td>104</td>
</tr>
<tr>
<td>Configure History Record Retention</td>
<td>104</td>
</tr>
<tr>
<td>Superclustering</td>
<td>106</td>
</tr>
<tr>
<td>About Superclustering</td>
<td>106</td>
</tr>
<tr>
<td>Verify DNS FQDN Resolution</td>
<td>107</td>
</tr>
<tr>
<td>View Details for RealPresence DMA Systems</td>
<td>107</td>
</tr>
<tr>
<td>Create or Join a Supercluster</td>
<td>107</td>
</tr>
<tr>
<td>Organize Territories and Assign Responsibilities</td>
<td>109</td>
</tr>
<tr>
<td>Busy Out a Cluster</td>
<td>109</td>
</tr>
<tr>
<td>Stop Using a Cluster</td>
<td>110</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Start Using a Cluster</td>
<td>110</td>
</tr>
<tr>
<td>Remove a Cluster From a Supercluster</td>
<td>111</td>
</tr>
<tr>
<td><strong>External Device Configuration</strong></td>
<td>112</td>
</tr>
<tr>
<td><strong>External H.323 Gatekeepers</strong></td>
<td>113</td>
</tr>
<tr>
<td>View External Gatekeepers</td>
<td>113</td>
</tr>
<tr>
<td>Add an External Gatekeeper</td>
<td>113</td>
</tr>
<tr>
<td>Edit an External Gatekeeper</td>
<td>115</td>
</tr>
<tr>
<td>Add an External Gatekeeper With Both an IPv4 and IPv6 Address</td>
<td>116</td>
</tr>
<tr>
<td><strong>External SIP Peers</strong></td>
<td>117</td>
</tr>
<tr>
<td>Multiple External SIP Peers</td>
<td>117</td>
</tr>
<tr>
<td>SIP Peer Availability and Third-Party Network Devices</td>
<td>117</td>
</tr>
<tr>
<td>View External SIP Peers</td>
<td>118</td>
</tr>
<tr>
<td>Add an External SIP Peer</td>
<td>118</td>
</tr>
<tr>
<td>Edit an External SIP Peer</td>
<td>124</td>
</tr>
<tr>
<td>SIP Peer Postliminary Output Format Options</td>
<td>129</td>
</tr>
<tr>
<td>To Header Format Options</td>
<td>130</td>
</tr>
<tr>
<td>Request-URI Header Format Options</td>
<td>130</td>
</tr>
<tr>
<td>Free Form Template Variables</td>
<td>131</td>
</tr>
<tr>
<td>To Header and Request-URI Header Examples</td>
<td>132</td>
</tr>
<tr>
<td>Add an Authentication Credential Entry</td>
<td>133</td>
</tr>
<tr>
<td>Edit an Authentication Credential Entry</td>
<td>133</td>
</tr>
<tr>
<td>Add an External Registration</td>
<td>134</td>
</tr>
<tr>
<td>Edit an External Registration</td>
<td>135</td>
</tr>
<tr>
<td><strong>External H.323 Session Border Controllers</strong></td>
<td>137</td>
</tr>
<tr>
<td>View External H.323 SBCs</td>
<td>137</td>
</tr>
<tr>
<td>Add an External H.323 SBC</td>
<td>138</td>
</tr>
<tr>
<td>Edit an External H.323 SBC</td>
<td>139</td>
</tr>
<tr>
<td><strong>External Skype for Business Systems</strong></td>
<td>141</td>
</tr>
<tr>
<td>View External Skype for Business Systems</td>
<td>141</td>
</tr>
<tr>
<td>Add an External Skype System</td>
<td>142</td>
</tr>
<tr>
<td>Edit an External Skype System</td>
<td>144</td>
</tr>
</tbody>
</table>
## MCU Management

Section 1: Configuring a Polycom MCU for use with the RealPresence DMA System
- Configure Compatible Security Settings
- Configure User Connections
- Disable Automatic Password Generation
- Configure SIP Settings

Section 2: Configuring a Cisco MCU for use with the Polycom® RealPresence® DMA® System
- Disable Media Port Reservations
- Using ISDN Gateways
- ISDN Gateway Selection Process
- Bandwidth Management

## MCUs

- View the MCUs List
- View MCU Details
- Add an MCU
- Edit an MCU
- Add a Session Profile
- Edit a Session Profile
- Delete an MCU
- Stop Using an MCU
- Start Using an MCU Again
- Busy Out an MCU
- Quarantine an MCU
- Unquarantine an MCU
- Block Registrations From an MCU
- Unblock Registrations From an MCU
- View Call History

## MCU Pools and Pool Orders

- MCU Selection Process
- MCU Availability and Reliability Tracking
- Working with MCU Pools
  - View MCU Pools
  - Add an MCU Pool
  - Edit an MCU Pool
  - Delete an MCU Pool
- Working with MCU Pool Orders
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Naming Conventions for Pool Orders</td>
<td>167</td>
</tr>
<tr>
<td>View MCU Pool Orders</td>
<td>167</td>
</tr>
<tr>
<td>Add an MCU Pool Order</td>
<td>168</td>
</tr>
<tr>
<td>Edit an MCU Pool Order</td>
<td>168</td>
</tr>
<tr>
<td>Edit the Priority Ranking of a Pool Order</td>
<td>169</td>
</tr>
<tr>
<td>Delete an MCU Pool Order</td>
<td>169</td>
</tr>
<tr>
<td><strong>Integration with Other Services</strong></td>
<td>170</td>
</tr>
<tr>
<td><strong>Microsoft® Active Directory® Integration</strong></td>
<td>171</td>
</tr>
<tr>
<td>Integrate with Active Directory</td>
<td>171</td>
</tr>
<tr>
<td>Understanding Base DN</td>
<td>174</td>
</tr>
<tr>
<td>Adding Passcodes for Enterprise Users</td>
<td>175</td>
</tr>
<tr>
<td>Generate Chairperson and Conference Passcodes for Enterprise Users</td>
<td>176</td>
</tr>
<tr>
<td>Active Directory Cache Refresh Frequency</td>
<td>177</td>
</tr>
<tr>
<td>Orphaned Groups and Users</td>
<td>177</td>
</tr>
<tr>
<td>Generate an Orphaned Groups and Users Report</td>
<td>178</td>
</tr>
<tr>
<td>Remove Orphaned Groups and Users</td>
<td>178</td>
</tr>
<tr>
<td>About the System’s Directory Queries</td>
<td>179</td>
</tr>
<tr>
<td>User Search</td>
<td>179</td>
</tr>
<tr>
<td>Group Search</td>
<td>180</td>
</tr>
<tr>
<td>Global Group Membership Search</td>
<td>180</td>
</tr>
<tr>
<td>Attribute Replication Search</td>
<td>180</td>
</tr>
<tr>
<td>Configurable Attribute Domain Search</td>
<td>181</td>
</tr>
<tr>
<td>Domain Search</td>
<td>181</td>
</tr>
<tr>
<td>Service Account Search</td>
<td>181</td>
</tr>
<tr>
<td>View the Active Directory Page</td>
<td>182</td>
</tr>
<tr>
<td><strong>Microsoft Exchange Server Integration</strong></td>
<td>187</td>
</tr>
<tr>
<td>Polycom Solution and Integration Support</td>
<td>187</td>
</tr>
<tr>
<td>Differences Between Calendaring and Scheduling</td>
<td>188</td>
</tr>
<tr>
<td>Microsoft Exchange Server Page</td>
<td>188</td>
</tr>
<tr>
<td>Exchange Server Integration</td>
<td>188</td>
</tr>
<tr>
<td>Integrate the Polycom RealPresence DMA System with Your Exchange Server</td>
<td>189</td>
</tr>
<tr>
<td><strong>Microsoft® Skype® for Business Integration</strong></td>
<td>191</td>
</tr>
<tr>
<td>Lync 2013 vs. Skype for Business 2015 Integration</td>
<td>191</td>
</tr>
<tr>
<td>Scheduled Conferences with Polycom RealConnect™</td>
<td>192</td>
</tr>
<tr>
<td>Automatic Contact Creation and Configuration</td>
<td>193</td>
</tr>
<tr>
<td>Active Directory Service Account Permissions</td>
<td>193</td>
</tr>
</tbody>
</table>
Contents

Polycom, Inc. 11

Change a Conference Template’s Priority ............................................. 237
Delete a Conference Template .............................................................. 238

IVR Prompt Sets .............................................................................. 239
View an IVR Prompt Set .................................................................. 240
Add a Custom IVR Prompt Set ............................................................ 241

Shared Number Dialing .................................................................. 242
View Virtual Entry Queues ............................................................... 244
Add a Virtual Entry Queue ............................................................... 244
Add a Direct Dial Virtual Entry Queue ............................................. 246
Edit a Virtual Entry Queue ............................................................... 246
Edit a Direct Dial Virtual Entry Queue ............................................. 248
Test Script Debugging for VEQ Scripts ............................................ 249
Sample Virtual Entry Queue Script .................................................... 249

SIP Conference Factories ................................................................. 251
Working with SIP Conference Factories ............................................. 251
Add a SIP Conference Factory ....................................................... 251
Edit a SIP Conference Factory ........................................................ 252
Delete a SIP Conference Factory ...................................................... 253

Presence Publishing for Skype ......................................................... 254
Configure Presence Publishing for Skype ........................................ 254
Remove Contacts from Active Directory ....................................... 256
Recreate Skype Contact Resources ............................................... 257

Call Server Configuration ................................................................. 258

Call Server Settings ......................................................................... 259
Configure the Call Server ................................................................. 259

Dial Plans ......................................................................................... 264
Dial Rules ......................................................................................... 264
Default Dial Plan ............................................................................. 265
   Suggestions for Modifying the Default Dial Plan ......................... 266
Add a Dial Plan ............................................................................... 268
Add a Dial Rule to a Dial Plan ....................................................... 268
Edit a Dial Rule ............................................................................... 273
Associating a Dial Plan to a Call Service ....................................... 274
Associate a Dial Plan to SIP Service ............................................... 274
## Contents

Edit Device Authentication ............................... 312

### Site Topology ........................................ 314

#### Site Topology ........................................ 315
   - Shared Site Topology for Integrated Polycom Systems .............................. 315
   - Bandwidth Management ................................ 315
   - Cascade for Bandwidth Conferences ..................................................... 316
   - Supercluster Assignments ................................................................. 316
   - Configure Site Topology ............................................................... 316
   - Embedded DNS .......................................................... 318
      - Enable DNS Publishing .......................................................... 319

#### Working with Site Topology ........................... 320
   - Sites .......................................................... 320
      - View the Site List ......................................................... 320
      - View the Site Information ............................................... 321
      - Add a Site ................................................... 322
      - Edit a Site ................................................... 327
      - Add a Subnet .............................................. 331
      - Edit a Subnet .............................................. 331
   - Network Clouds .............................................. 332
      - View Network Clouds .............................................. 332
      - Add a Network Cloud .............................................. 332
      - Edit a Network Cloud .............................................. 333
   - Site Links .................................................... 334
      - Add a Site Link .................................................... 334
      - Edit a Site Link .................................................... 335
   - Site-to-Site Exclusions .............................................. 336
      - View Site-to-Site Exclusions .............................................. 336
      - Add a Site-to-Site Exclusion .............................................. 336
   - Territories ..................................................... 336
      - View the Territories List ..................................................... 337
      - Add a Territory ..................................................... 337
      - Edit a Territory ..................................................... 338

#### Users and Groups ...................................... 340

#### User Roles and Access Privileges ........................ 341
   - User Roles ..................................................... 341
## Maintenance

### System Management and Maintenance

- Administrator Responsibilities
- Administrator Best Practices
- Auditor Responsibilities
- Auditor Best Practices
- Provisioner Responsibilities

**Recommended Regular Maintenance**

- Archive Backups
- Check General System Health and Capacity
- Check Microsoft Active Directory Health
- Check Security Configuration
- Check Certificates
- Check Network Usage Data Export
- CDR Export

### System Log Files

- Working With System Logs
- Manually Roll the System Logs
- Download Active Logs
- Download an Individual Log File
- Download Archived Logs
- Delete a System Log Archive

### Backing Up and Restoring

- Backing Up Your System
- View Locally Stored Backup Files
- Create a New Backup File
- Download a Backup File
- Upload a Backup File
- Configure Remote Backup Settings

**Restoring Your System**

- Restore from a Backup File on the Cluster
- Restore from a Backup File on the Polycom RealPresence DMA System’s USB Flash Drive

### Upgrading the Software

- Upgrading Overview
- Upgrading Preparation
View Software Upgrade Information .............................................. 401
Upload the Upgrade Package ...................................................... 401
Prepare Your Supercluster ......................................................... 401
Basic Upgrade Procedure .......................................................... 402
Upgrade the Software .............................................................. 402
Perform a Minor or Major Upgrade on a Superclustered System ........ 403
Upgrade a Supercluster During a Complete Service Outage .............. 404
Upgrading a Supercluster While Maintaining Partial Service .......... 406
Factors to Consider for an Incremental Supercluster Upgrade ......... 406
Rolling Back System Software to Previous Versions ...................... 407
Roll Back an Upgrade ................................................................. 408

Shutting Down and Restarting ................................................... 410
Restart or Shut Down One or Both Servers in a Cluster .................. 410
Start Up a Shut-Down Cluster .................................................... 411

Monitoring ................................................................. 412

Active Calls ................................................................. 413
View the Active Calls List .......................................................... 413
View Call Details ................................................................. 414

Endpoints ................................................................. 417
Monitor Endpoints ................................................................. 417
Add an Endpoint ................................................................. 420
Edit an Endpoint ................................................................. 421
Edit Multiple Endpoints .......................................................... 423
Delete an Endpoint ............................................................... 423
Add an Alias ................................................................. 424
Edit an Alias ................................................................. 424
Associate a User With a Device ................................................. 424
Disassociate a User From an Endpoint ...................................... 424
Block Registrations From an Endpoint ...................................... 425
Unblock Registrations From an Endpoint .................................. 425
Quarantine an Endpoint ......................................................... 426
Unquarantine an Endpoint ..................................................... 426
Names and Aliases in a Mixed H.323 and SIP Environment .......... 426
Naming ITP Systems for Recognition by the Polycom RealPresence DMA System ........................................... 427
<table>
<thead>
<tr>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property Changes ........................................... 447</td>
</tr>
<tr>
<td>Registration History ........................................ 447</td>
</tr>
<tr>
<td>View the Registration History .............................. 447</td>
</tr>
<tr>
<td>Call Detail Records .......................................... 448</td>
</tr>
<tr>
<td>Export CDR Data ................................................ 449</td>
</tr>
<tr>
<td>Call Record Layouts .......................................... 449</td>
</tr>
<tr>
<td>Conference Record Layouts .................................. 454</td>
</tr>
<tr>
<td>Network Usage Report ......................................... 455</td>
</tr>
<tr>
<td>Export Network Usage Data .................................... 456</td>
</tr>
<tr>
<td>View Network Usage Data ...................................... 456</td>
</tr>
<tr>
<td>Conference Room Errors Report ............................. 459</td>
</tr>
<tr>
<td>Export Conference Room Errors Data ........................ 460</td>
</tr>
<tr>
<td>Enterprise Passcode Errors Report ......................... 461</td>
</tr>
<tr>
<td>Export Enterprise Passcode Errors Data .................... 462</td>
</tr>
<tr>
<td>Troubleshooting ................................................ 463</td>
</tr>
<tr>
<td>Alerts ............................................................ 464</td>
</tr>
<tr>
<td>Supercluster Status .......................................... 465</td>
</tr>
<tr>
<td>Alert 1001 ....................................................... 465</td>
</tr>
<tr>
<td>Alert 1002 ....................................................... 465</td>
</tr>
<tr>
<td>Alert 1003 ....................................................... 465</td>
</tr>
<tr>
<td>Alert 1004 ....................................................... 465</td>
</tr>
<tr>
<td>Territory Status ................................................ 466</td>
</tr>
<tr>
<td>Alert 1103 ....................................................... 466</td>
</tr>
<tr>
<td>Alert 1105 ....................................................... 466</td>
</tr>
<tr>
<td>Alert 1106 ....................................................... 466</td>
</tr>
<tr>
<td>Alert 1107 ....................................................... 467</td>
</tr>
<tr>
<td>Alert 1108 ....................................................... 467</td>
</tr>
<tr>
<td>Asynchronous Operation ....................................... 467</td>
</tr>
<tr>
<td>RealPresence Resource Manager System Integration ........ 467</td>
</tr>
<tr>
<td>Alert 2001 ....................................................... 468</td>
</tr>
<tr>
<td>Alert 2002 ....................................................... 468</td>
</tr>
<tr>
<td>Alert 2004 ....................................................... 468</td>
</tr>
<tr>
<td>Active Directory Integration ................................. 468</td>
</tr>
<tr>
<td>Alert 2101 ....................................................... 468</td>
</tr>
<tr>
<td>Alert 2102 ....................................................... 469</td>
</tr>
<tr>
<td>Alert 2104 ....................................................... 469</td>
</tr>
</tbody>
</table>
Alert 3309 ......................................................... 478
Alert 3310 ......................................................... 478
Server Resources ................................................... 478
Alert 3401 ......................................................... 478
Alert 3403 ......................................................... 479
Alert 3404 ......................................................... 479
Alert 3405 ......................................................... 479
Alert 3406 ......................................................... 479
Data Synchronization ............................................... 480
Alert 3601 ......................................................... 480
Alert 3602 ......................................................... 480
Alert 3603 ......................................................... 480
Alert 3604 ......................................................... 480
Alert 3605 ......................................................... 481
Alert 3606 ......................................................... 481
System Health and Availability ................................. 481
Alert 3801 ......................................................... 481
Alert 3802 ......................................................... 481
Alert 3803 ......................................................... 482
Cluster Features ................................................... 482
Alert 3901 ......................................................... 482
Alert 3902 ......................................................... 482
Alert 3903 ......................................................... 482
Alert 3904 ......................................................... 483
Alert 3905 ......................................................... 483
MCUs ............................................................... 483
Alert 4001 ......................................................... 483
Alert 4002 ......................................................... 483
Alert 4003 ......................................................... 484
Alert 4004 ......................................................... 484
Alert 4005 ......................................................... 484
Alert 4009 ......................................................... 484
Alert 4010 ......................................................... 485
Alert 4011 ......................................................... 485
Alert 4012 ......................................................... 485
Alert 4013 ......................................................... 485
Alert 4014 ......................................................... 486
Alert 4015 ......................................................... 486
Alert 4016 ......................................................... 486
Alert 4017 ......................................................... 486
<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run SAR</td>
<td>496</td>
</tr>
<tr>
<td>Check NTP Status</td>
<td>496</td>
</tr>
<tr>
<td>Manually Synchronize all Clusters</td>
<td>496</td>
</tr>
<tr>
<td>Reset to Default Settings</td>
<td>497</td>
</tr>
<tr>
<td>Diagnostics for your Polycom Server</td>
<td>498</td>
</tr>
</tbody>
</table>
Getting Started

This section provides an introduction to the Polycom® RealPresence® DMA® system features and initial configuration. It includes:

- Polycom® RealPresence® DMA® System Overview
- Working in the Polycom® RealPresence® DMA® System
- Initial System Configuration
Polycom® RealPresence® DMA® System Overview

The Polycom® RealPresence® Distributed Media Application™ (DMA®) system is a highly reliable and scalable video collaboration infrastructure solution. The following topics introduce you to the system:

- The Polycom RealPresence DMA System’s Primary Functions
- The Polycom RealPresence DMA System’s Three Configurations
- Polycom Solution Support

The Polycom RealPresence DMA System’s Primary Functions

The Polycom RealPresence DMA system provides the following primary functions:

- Conference Manager
- Call Server
- RealPresence® Platform API
- SVC Conferencing Support

Conference Manager

The Polycom RealPresence DMA system’s Conference Manager facilitates multipoint video conferencing. A multipoint video conference is one in which multiple endpoints are connected, with all participants able to see and hear each other. The endpoints connect to a media server (Multipoint Control Unit, or MCU), which processes the audio and video from each and sends the conference audio and video streams back to them.

Traditionally, such multipoint conferences had to be scheduled in advance, reserving ports on a specific MCU, in order to ensure the availability of resources. Conference Manager makes this unnecessary. Conference Manager uses advanced routing policies to distribute voice and video calls among multiple MCUs, creating a single virtual resource pool. This greatly simplifies multipoint video conferencing resource management and uses MCU resources more efficiently.

The Polycom RealPresence DMA system integrates with your Microsoft® Active Directory®, automating the task of provisioning users with virtual meeting rooms (VMRs), which are available for use at any time for multipoint video conferencing. Combined with its advanced resource management, this makes reservationless (ad hoc) video conferencing on a large scale feasible and efficient, reducing or eliminating the need for conference scheduling.

The Polycom RealPresence DMA system’s ability to handle multiple MCUs as a single resource pool makes multipoint conferencing services highly scalable. You can add MCUs on the fly without impacting end users and without requiring re-provisioning. The RealPresence DMA system can span a conference across two
or more MCUs (called cascading), enabling the conference to contain more participants than any single MCU can accommodate.

The Conference Manager continually monitors the resources used and available on each MCU and intelligently distributes conferences among them. If an MCU fails, loses its connection to the system, or is taken out of service, the Polycom RealPresence DMA system distributes new conferences to the remaining MCUs. Every conference on the failed MCU is restarted on another MCU (provided there is space available). The consequences for existing calls in those conferences depend on whether they’re H.323 or SIP:

- H.323 participants are not automatically reconnected to the conference. In order to rejoin the conference, dial-in participants simply need to redial the same number they used for their initial dial-in. Dial-out participants will need to be dialed out to again; the RealPresence DMA system doesn’t automatically redial out to them.
- SIP participants are automatically reconnected to the conference on the new MCU. This includes both dial-in and dial-out SIP participants. No new dial-out is needed because the RealPresence DMA system maintains the SIP call leg to the participant and only has to re-establish the SIP call leg from the RealPresence DMA system to the MCU.

**Call Server**

The Polycom RealPresence DMA system’s Call Server provides the following functionality:

- H.323 gatekeeper
- SIP registrar and proxy server
- H.323 <-> SIP transition gateway
- Dial plan and prefix services
- Device authentication
- Bandwidth management

**RealPresence® Platform API**

The Polycom RealPresence DMA system optionally allows an API client application, developed by you or a third party, to access the Polycom RealPresence® Platform Application Programming Interface (API). The API provides programmatic access to the Polycom RealPresence DMA system for the following:

- Provisioning
- Conference control and monitoring
- Call control and dial-out
- Billing and usage data retrieval
- Resource availability queries

The API uses XML or JSON encoding over HTTPS transport and adheres to a Representational State Transfer (REST) architecture.

**Note:** The API communicates asynchronously. Clients subscribing to event notifications via the API must be prepared to receive notifications out of order.
A Polycom RealPresence Resource Manager system can integrate with the RealPresence DMA system via the API. The API provides the full programmatic access to the RealPresence DMA system described above and enables users of the RealPresence Resource Manager scheduling interface to:

- Schedule conferences using the RealPresence DMA system's MCU resources.
- Set up Anytime conferences. Anytime conferences are referred to as preset dial-out conferences in the RealPresence DMA system.

**SVC Conferencing Support**

The Polycom RealPresence DMA system supports the Annex G extension of the H.264 standard, known as H.264 Scalable Video Coding (SVC), for both point-to-point and multipoint (VMR) calls.

SVC is sometimes referred to as layered media because the video streams consist of a base layer that encodes the lowest available quality representation plus one or more enhancement layers that each provide an additional quality improvement. SVC supports three dimensions of scalability: temporal (frames per second), spatial (resolution and aspect ratio), and quality (signal-to-noise ratio).

The video stream to a device can be tailored to fit the bandwidth available and device capabilities by adjusting the number of enhancement layers sent to the device.

For multipoint conferencing, the MCU doesn't have to do processing-intensive mixing and transcoding to optimize the experience for each device. Instead, it simply passes the video stream from each device to each device, including the enhancement layers that provide the best quality the device can support.

Polycom’s SVC solution focuses on the temporal and spatial dimensions. It offers a number of advantages over standard AVC conferencing, including:

- Improved video quality at lower bandwidths
- Improved audio and video error resiliency (good audio quality with more than 50% packet loss, good video quality with more than 25% packet loss)
- Lower end-to-end latency (typically less than half that of AVC)
- More efficient use of bandwidth
- Lower infrastructure cost and operational expenses
- Easier to provision, control, and monitor
- Better security (end-to-end encryption)

Polycom’s SVC solution is supported by the Polycom RealPresence Platform and Environments, including the latest generation of Polycom MCUs and RealPresence room, personal, desktop, and mobile endpoints. Existing RMX MCUs with MPMx cards can be made SVC-capable with a software upgrade, and doing so triples their HD multipoint conferencing capacity.

RealPresence Collaboration Server 800s MCUs support mixed-mode (SVC+AVC) conferences. Both SVC and AVC endpoints can join the conference, and each gets the appropriate experience: SVC endpoints get SVC mode and get a video stream for each AVC participant; AVC endpoints get a single Continuous Presence (CP) video stream of the participants (both AVC and SVC) supplied by the MCU.

When the Polycom RealPresence DMA system selects an MCU that doesn’t support SVC for a conference configured for mixed mode, it starts the conference as an AVC-only conference (all SVC-capable endpoints also support AVC). But if the MCU supports SVC but not mixed mode (RMX 7.8), the conference fails to start.
Refer to your RealPresence Collaboration Server or RMX documentation for important information about the MCU’s implementation of SVC conferencing and its configuration, limitations, and constraints.

The Polycom RealPresence DMA System’s Three Configurations

Depending on your organization’s needs, you can deploy the Polycom RealPresence DMA system in one of the following three configurations.

- Two-server Configuration
- Single-server Configuration
- Supercluster Configuration

Two-server Configuration

The Polycom RealPresence DMA system is designed to be deployed as a pair of co-located redundant servers that share the same virtual IP address(es). The two-server cluster configuration of the Polycom RealPresence DMA system has no single point of failure within the system that could cause the service to become unavailable.

The two servers communicate with the public and/or private network that connects them. To determine which one should host the public virtual IP address, each server uses three criteria:

- Ability to ping its own public physical address
- Ability to ping the other server’s public physical address
- Ability to ping the default gateway

In the event of a tie, the server already hosting the public virtual address wins.

Failover to the backup server takes about five seconds in the event of a graceful shutdown and about 40 seconds in the event of a power loss or other failure. In the event of a single server failure, these things happen:

- All calls that are being routed through the failed server are terminated (including SIP calls, VMR calls, and routed mode H.323 calls). These users simply need to redial the same number, and they are placed back into conference or reconnected to the point-to-point call they were in. The standby server takes over the virtual signaling address, so existing registrations and new calls are unaffected.
- Direct mode H.323 point-to-point calls are not dropped, but the bandwidth management system loses track of them. This could result in overuse of the available network bandwidth.
- If the failed server is the active web host for the system’s management interface, the active user interface sessions end, the web host address automatically migrates to the remaining server, and it becomes the active web host. Administrative users can then log back into the system at the same URL. The system can always be administered via the same address, regardless of which server is the web host.

The internal databases within each Polycom RealPresence DMA system server are fully replicated to the other server in the cluster. If a catastrophic failure of one of the database engines occurs, the system automatically switches itself over to use the database on the other server.
**Single-server Configuration**

The Polycom RealPresence DMA system can also be deployed in a single-server configuration. This configuration offers all the advantages of the Polycom RealPresence DMA system except the redundancy and fault tolerance. It can be upgraded to a two-server cluster at any time.

The *Polycom RealPresence DMA System Operations Guide* and online help generally assume a redundant two-server cluster. Where there are significant differences between the two configurations, those are spelled out.

**Supercluster Configuration**

To provide geographic redundancy and better network traffic management, up to 10 geographically distributed Polycom RealPresence DMA system clusters (two-server or single-server) can be integrated into a supercluster. All five clusters can be Call Servers (function as gatekeeper, SIP proxy, SIP registrar, and gateway). Up to three can be designated as Conference Managers (manage an MCU resource pool to host conference rooms).

The superclustered Polycom RealPresence DMA systems can be centrally administered and share a common data store. Each cluster maintains a local copy of the data store, and changes are replicated to all the clusters. Most system configuration is supercluster-wide. The exceptions are cluster-specific or server-specific items like network settings and time settings.

**Clusters versus Superclusters**

Technically, a standalone Polycom RealPresence DMA system (two-server or single-server) is a supercluster that contains one cluster. All the system configuration and other data that is shared across a supercluster is kept in the same data store. At any time, another Polycom RealPresence DMA system can be integrated with it to create a two-cluster supercluster that shares its data store.

It is important to understand the difference between two co-located servers forming a single RealPresence DMA system (cluster) and two geographically distributed RealPresence DMA system clusters (single-server or two-server) joined into a supercluster.

A single two-server cluster has the following characteristics:

- A single shared virtual IP address and FQDN, which switches from one server to the other when necessary to provide local redundancy and fault tolerance.
- A single management interface and set of local settings.
- Ability to manage a single territory, with no territory management backup.
- A single set of Call Server and Conference Manager responsibilities.

A supercluster consisting of two clusters (single-server or two-server) has the following characteristics:

- Separate IP addresses and FQDNs for each cluster.
- Separate management interfaces and sets of local settings for each cluster.
- Ability for each cluster to manage its own territory, with another cluster able to serve as backup for that territory.
- Different Call Server and Conference Manager responsibilities for each territory and thus each cluster.
Polycom Solution Support

Polycom Implementation and Maintenance services provide support for Polycom solution components only. Additional services for supported third-party Unified Communications (UC) environments integrated with Polycom solutions are available from Polycom Global Services and its certified Partners. These additional services will help customers successfully design, deploy, optimize, and manage Polycom visual communications within their UC environments.

Professional Services for Microsoft Integration are mandatory for Polycom Conferencing for Microsoft Outlook® and Microsoft Office Communications Server, Lync® 2010 Server, Lync Server, or Skype® for Business Server integrations. For more information, please visit www.polycom.com/services/professional_services/ or contact your local Polycom representative.
Working in the Polycom® RealPresence® DMA® System

You can configure and manage the Polycom® RealPresence® DMA® system by using the management user interface. Its Dashboard and menus provide access to Call Server and Conference Manager functions. The following topics include some general information you should know when working in the RealPresence DMA system.

- Log In to the System
- Sign Out of the System
- Change Your Password
- Dashboard
- Customize Your Dashboard
- View System Alerts
- Refreshing Data
- Field Input Requirements
- System Ports

Log In to the System

You need to log in to the management user interface from a client system with a browser that supports HTML5.

Most browsers provide options to save login credentials for applications or websites you access. Browsers may also "auto-complete" field information you have previously entered, including user names and passwords. To increase the security of your RealPresence DMA system, Polycom recommends that you disable any saved credentials or auto-complete options in your browser settings.

To log in to the RealPresence DMA system:

1. Point your browser to the host name or IP address of your system.
2. Enter your username and password and click Log In.
   The RealPresence DMA system dashboard displays.

Sign Out of the System

You can sign out of the RealPresence DMA system from the dashboard.
To sign out of the system:

» Click and select Sign Out.

Change Your Password

You can configure the system to expire local user passwords after a certain number of days. If your password has expired, the system prompts you for a new password when you try to sign in to the management user interface.

You can change your password at other times, as well.

To change your password:

1. Click and select Change Password.
2. Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>The user name with which you’re logging in. Display only.</td>
</tr>
<tr>
<td>Old password</td>
<td>For security reasons, you must re-enter your old password.</td>
</tr>
<tr>
<td>New password</td>
<td>Enter a new password. The password must satisfy the local password rules specified for the system (see Configure Local Password Settings).</td>
</tr>
<tr>
<td>Confirm new password</td>
<td>Retype the password to confirm that you entered it correctly.</td>
</tr>
</tbody>
</table>

3. Click OK.

Dashboard

When you log into the RealPresence DMA system, the system Dashboard displays. You can use the system Dashboard to view information about system health and activity levels.

To return to the Dashboard from any other page, click the Polycom logo to the left of the menus.

Dashboard Panes

Dashboard panes provide details about numerous RealPresence DMA system functions. You can open more than one instance of any pane.

Active Directory Integration Pane

Displays information about the status of Active Directory integration. If the system is integrated with AD, this pane shows:

- The territory (and cluster) responsible for refreshing the cache.
- When the cache was last refreshed and by which server.
- The AD server address and user ID used.
• The number of enterprise conference rooms created.

Click Link to go to the Microsoft Active Directory page.

**Call Server Active Calls Pane**

Displays the current number of calls in total and for each system in the supercluster, and the licensed call limit in total and for each system.

In a superclustered environment, a call may span multiple clusters. Each “leg” of such a call is counted on the cluster it is on. The total for all clusters includes the total of all legs of cluster-spanning calls. Also, any confirmed ARQ request that originated from an MCU consumes a license on the cluster that confirms it.

If H.323 signaling is enabled, the call mode (direct or routed) is also shown.

Click a column heading to sort on that column. Click the link icon to go to the Active Calls page.

**Call Server Registrations Pane**

Displays the total number of active (including active quarantined) and inactive (including inactive quarantined and blocked) endpoint registrations and the number that failed in the past 24 hours. Hover over a registration number to see the limit.

Also displays the total number of registrations for each cluster of the supercluster. Hover over a cluster’s total to see the breakdown between active and inactive.

Click a column heading to sort on that column. Click the link icon to go to the Endpoints page.

**Cluster Info Pane**

Displays detailed information about the selected cluster. For a two-server cluster, the pane contains a tab for each server. The tab label indicates which server is currently active. Each tab contains the following information about the server:

• Current date, time, and uptime
• System version number
• Hardware model and serial number
• Time source
• Management network MAC and physical and virtual IPv4 and IPv6 addresses
• Signaling network MAC and physical and virtual IPv4 and IPv6 addresses
• CPU utilization percentage (all cores)
• System memory usage (it’s normal for memory usage to be high)
• Swap space (total and free)
• Disk space usage (actual and percentage)
• Log space usage (actual and percentage) and next scheduled log purge

**Conference History – Max Participants Pane**

Displays a bar graph showing variations in the maximum number of Conference Manager conference participants over the time span you select.
The graph shows the data for all Conference Manager clusters. The Ad-hoc participants category includes all dial-outs and all dial-ins to non-scheduled conferences. The Other participants category includes all dial-ins to conferences scheduled via Polycom Conferencing for Outlook (calendared conferences) or via an API client such as the Polycom RealPresence Resource Manager system.

Click the link icon to go to the Conference History page.

### Conference Manager MCUs Pane

Displays information about all MCUs that are managed by the Conference Manager to host conference rooms (virtual meeting rooms, or VMRs).

The information shown includes the MCU’s connection and service status, its capabilities, its reliability (disconnects and call failures), and the number of ports in use and available to Conference Manager.

Hover over an icon to see an explanation of it. Click the Link button to go to the MCUs page.

**Note:** An MCU may be connected to up to three Conference Manager clusters. If one of the three Conference Managers loses its connection to the MCU, this is counted as 0.33 disconnects. If all connections to the MCU are lost, this is counted as 1 disconnect.

### Conference Manager Usage Pane

Displays usage information for Conference Manager, either for all Conference Manager clusters or for the selected cluster.

The information shown includes the territories for which Conference Manager is enabled, the number of conferences and participants, the port usage, and the number of local users and custom conference rooms.

**Note:** The RealPresence DMA system reports port numbers based on CIF resource usage. Version 8.1 and later Polycom MCUs report HD720p30 port numbers. In general, 3 CIF = 1 HD720p30, but it varies depending on bridge/card type and other factors.

See your Polycom RMX or RealPresence Collaboration Server documentation for more detailed information about resource usage.

### Exchange Server Integration Pane

If the Polycom RealPresence DMA system is integrated with a Microsoft Exchange server, displays the following:

- The server in the cluster performing Exchange server integration and integration status, which can be one of the following:
  - **Unavailable** — A service status or inter-server communication problem prevented determination of the integration status.
  - **Error** — The system was unable to establish a connection to the Exchange server. This could be a network or Exchange server problem, or it could be a login failure.
  - **Awaiting Active Directory** — The system isn't integrated with the Active Directory, required for Exchange server integration.
  - **Primary SMTP mailbox not found** — The mailbox configured for the Polycom RealPresence DMA system isn’t in the system’s Active Directory cache.
Working in the Polycom® RealPresence® DMA® System

- **Subscription pending** — The Polycom RealPresence DMA system has asked the Exchange server to send it notifications and is waiting to receive its first notification to confirm that the Exchange server can communicate with the system. If this status persists for more than a minute or so, there is likely a configuration problem (such as an invalid certificate or the Exchange server is unable to resolve the RealPresence DMA system’s FQDN).

- **Exchange authentication failed** — The credentials for the Polycom RealPresence DMA system’s mailbox are no longer valid (e.g., the password has expired).

- **OK** — The Polycom RealPresence DMA system is receiving and processing Polycom Conferencing meeting notifications from the Exchange server.

  - The territory configured for Exchange server integration, color-coded according to supercluster status.
  - The host name or IP address for the Exchange server as entered on the Microsoft Exchange Server page.
  - The Polycom RealPresence DMA system’s mailbox address.
  - The number of Polycom Conferencing meetings today.

Click the **Link** button to go to the Microsoft Exchange Server page.

**High Availability Status Pane**

If two RealPresence DMA systems are configured in High Availability mode, the pane displays the following:

  - Local physical IP address of the interface that is assigned the management service, HA connection status, VIP owner status.
  - Peer physical IP address of the interface that is assigned the management service, HA connection status, VIP owner status.
  - Status of each network interface enabled as an HA link or that has a virtual IP address (Up or Down).
  - Virtual IP address for the interface (if services are assigned to it).
  - Whether the HA network interfaces are connected (peer-to-peer) via crossover cable.

**RealPresence Resource Manager System Integration Pane**

If the Polycom RealPresence DMA system is integrated with a Polycom RealPresence Resource Manager system, displays the following:

  - Host name or IP address of the RealPresence Resource Manager system.
  - User name used to log into the RealPresence Resource Manager system.
  - Time when site topology data was last updated from the RealPresence Resource Manager system.
  - Number of territories, sites, site links, and network (MPLS) clouds in the site topology data obtained from the RealPresence Resource Manager system.

Click the **Link** button to go to the RealPresence Resource Manager page.

**Server Interfaces Pane**

Displays the interfaces for the server and the services, if any, that are assigned to each interface.
Signaling Settings Pane
Displays the H.323, SIP, and WebRTC signaling settings for the selected cluster, including whether each is enabled and what ports are assigned.
Click the Link button to go to the Signaling Settings page.

Supercluster Status Pane
Displays the status of each server in every cluster of the supercluster, the status of its private, management, and signaling interfaces, and the territory for which it’s responsible. A territory is green if being managed by its primary cluster, yellow if being managed by its backup cluster, and red if it’s out of service (no cluster is managing it). Hover over a name or icon to see more details.
The icons in the Status column indicate the status of the server. Hover over an icon to see further details.
Click the Link button to go to the DMAs page.

 Territory Status Pane
Lists each territory, its capabilities, and the primary and backup cluster responsible for it. Hover over the territory name to see more details. The territories are color-coded, each color with its own tooltips:

- **Green**: Active on primary cluster - The primary cluster for the territory is in service. The backup cluster may or may not be assigned.
- **Yellow**: Indicates one of the following:
  - Active on primary cluster - The primary cluster for the territory is unreachable from some clusters including the backup cluster. The backup cluster is not in service or is not assigned.
  - Active on backup cluster - The primary cluster for the territory is not in service or not assigned, but the backup cluster is in service.
  - Active on both primary and backup clusters - The primary cluster for the territory is unreachable from some clusters including the backup cluster, and the backup cluster is in service. The ownership of the territory is split between the primary and backup clusters.
- **Red**: Indicates one of the following:
  - Not active; associated clusters not in service - A primary or backup cluster is assigned to the territory (or both), but neither the primary nor the backup cluster are in service.
  - Not active; no primary or backup cluster assigned - No clusters are assigned to the territory.
Hover over a cluster name to see more details. Note that a cluster is considered in service if it is reachable from the backup cluster, even it is unreachable from some of the other clusters. A cluster is considered not in service if it has been given the Stop Using command, is busied out, or is unreachable.
Hover over a capabilities icon to see details of the capability. Click a column heading to sort on that column.
Click the Link button to go to the Territories page.

User Login History Pane
Displays the following information about logins by your user ID:

- The server you’re currently logged in to.
- The time, date, server logged in to, and source (host name or IP address) of the last successful login (prior to your current session) by your user ID.
Customize Your Dashboard

You can customize your Dashboard to display panes that contain information about various system functions. Initially, the Dashboard contains six default panes. You can add other panes or close any that you do not want to view. You can also add multiple copies of the same pane, with each showing information for a different cluster. The maximum number of panes is 50.

The buttons on the right side of each pane’s title bar let you access help, go to a related page (where appropriate), maximize the pane to fill the window, restore it to its normal size, or close the pane. Hover over a button to see what it does.

Note that the RealPresence DMA system stores your Dashboard layout in your web browser’s cache. If you log in to the system from different devices, your Dashboard view may differ.

To customize your Dashboard:

1. Click Edit to enable the Dashboard editing options.
2. Select from the following:
   - Add – displays a list of panes you can add to the Dashboard.
   - Save – saves your changes to the Dashboard.
   - Auto-arrange – arranges the panes to best fit your browser window.
   - Restore Defaults – restores the Dashboard to the six default panes.
   - Cancel – cancels your changes.

View System Alerts

An alert icon appears in the main menu bar and displays the number of alerts, if any, currently affecting the system.

To view system alerts:

1. Click to display the current alerts.
2. Click on an alert link to display the area of the system affected by the alert.

Refreshing Data

Data within the RealPresence DMA system can be automatically refreshed on some pages in the management user interface and manually refreshed on all pages in the management user interface.

Set the Automatic Refresh Rate

Automatically refreshing the data on a page within the management user interface updates the data that display at an interval you define. You can set an automatic refresh rate of 5, 15, 30, 45 seconds, or 1 minute.
When the RealPresence DMA system refreshes data, it takes several seconds to collect the data and deliver it to the management user interface. The system collects data as quickly as possible, but if you set the refresh rate to 5 seconds, the data returned are not guaranteed to be 5 seconds old at the most.

Note that when you select a refresh rate on a given management user interface page, the rate will apply to all pages that have the automatic refresh feature. The rate will also persist for future logins if the same user logs in from the same computer, using the same web browser.

**To set the automatic refresh rate:**

1. Go to any RealPresence DMA system management user interface page that has the automatic refresh icon ( ).
2. Select **Settings** next to the automatic refresh icon and choose a refresh rate.

The data on the page will automatically refresh at the rate you selected.

**Refresh Data Manually**

You can manually refresh the data on a management user interface page at any time by clicking the manual or automatic refresh icon.

**To refresh data manually:**

1. Go to any RealPresence DMA system management user interface page that has the manual refresh icon ( ) or automatic refresh icon ( ) and click the icon.

The data on the page will refresh.

**Field Input Requirements**

While every effort was made to internationalize the Polycom RealPresence DMA system, not all system fields accept Unicode entries. If you work in a language other than English, be aware that some fields accept only ASCII characters.

For input fields that accept a SIP URI, the supported characters for the "userinfo" portion of the URI include:

- Alpha: a-z, A-Z
- Numeric: 0-9
- Escaped: %XX where X=0-9, A-F, a-f
- Other: -_!~*'();:@&=+$,

For input fields that accept an H.323 alias, the supported characters include:

- All ASCII characters in the ranges %x21-24, %x26-3F, %x41-7f
- % @ and values < %x21 can be escaped.
- Escaped: %XX where X=0-9, A-F, a-f
Web Browsers

When you access the management user interface, the browser you use stores the web page information in a temporary cache memory file. When you make certain changes to the RealPresence DMA system that cause a system restart or that alter a security certificate, you may need to refresh or reload your browser to update the management user interface before you log back in. You may also need to refresh your browser if you receive system errors while downloading log files.

If you refresh your browser and still see outdated information or cannot download log files in the RealPresence DMA system, you need to clear your browser’s cache. See the instructions for your specific browser.

System Ports

The following table lists the inbound ports that may be open on the Polycom RealPresence DMA system, depending on signaling and security settings, integrations, and system configuration.

Note that the DMA system’s ephemeral port range is 20000-35999 for communication with external SIP devices. The H.323 stack uses ephemeral ports from a different range.

**RealPresence DMASystem Inbound Ports**

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>TCP</td>
<td>SSH. Only available if Linux console access is enabled.</td>
</tr>
<tr>
<td>53</td>
<td>TCP/UDP</td>
<td>DNS. Only available if the embedded DNS server is enabled.</td>
</tr>
<tr>
<td>80</td>
<td>TCP</td>
<td>HTTP. Redirects to 443 (HTTP access is not allowed).</td>
</tr>
<tr>
<td>123</td>
<td>UDP</td>
<td>NTP. Only available if an NTP server is specified in Time Settings.</td>
</tr>
<tr>
<td>161</td>
<td>UDP</td>
<td>SNMP. Default port; can be changed or disabled.</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>HTTPS. Redirects to 8443.</td>
</tr>
<tr>
<td>1719</td>
<td>UDP</td>
<td>H.323 RAS. Default port; can be changed.</td>
</tr>
<tr>
<td>1720</td>
<td>TCP</td>
<td>H.323 H.225 signaling. Default port; can be changed.</td>
</tr>
<tr>
<td>5060</td>
<td>TCP/UDP</td>
<td>Unencrypted SIP. Default port; can be changed or disabled; additional unencrypted ports can be added.</td>
</tr>
<tr>
<td>5061</td>
<td>TCP</td>
<td>SIP TLS. Default port; can be changed; additional encrypted ports can be added.</td>
</tr>
<tr>
<td>5986</td>
<td>TCP/TLS</td>
<td>Used for WinRM 2.0 communication during Polycom contact creation in Active Directory.</td>
</tr>
<tr>
<td>8080</td>
<td>TCP</td>
<td>HTTP. Redirects to 8443. Used for uploading upgrade packages and backups. During upgrades, the progress page is served from this port.</td>
</tr>
<tr>
<td>8443</td>
<td>TCP</td>
<td>HTTPS. Management interface access.</td>
</tr>
</tbody>
</table>
The following table lists the remote ports to which the Polycom RealPresence DMA system may connect, depending on signaling and security settings, integrations, and system configuration.

**RealPresence DMA System Remote Ports**

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>TCP</td>
<td>HTTP. MCUs, Exchange Web Services (calendaring). Only used if unencrypted connections are enabled.</td>
</tr>
<tr>
<td>162</td>
<td>TCP/UDP</td>
<td>SNMP notifications (Traps or Informs). Used if SNMP is enabled and configured to send notifications, or if system is monitored with RealPresence Resource Manager or RealPresence Platform Director.</td>
</tr>
<tr>
<td>389</td>
<td>TCP</td>
<td>LDAP. Active Directory integration.</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>HTTPS. MCUs, Exchange Web Services (calendaring).</td>
</tr>
<tr>
<td>514</td>
<td>UDP</td>
<td>Log forwarding.</td>
</tr>
<tr>
<td>636</td>
<td>TCP</td>
<td>Microsoft Active Directory integration.</td>
</tr>
<tr>
<td>1718</td>
<td>UDP</td>
<td>H.323 RAS.</td>
</tr>
<tr>
<td>1719</td>
<td>UDP</td>
<td>H.323 RAS.</td>
</tr>
<tr>
<td>1720</td>
<td>TCP</td>
<td>H.323 H.225 signaling.</td>
</tr>
<tr>
<td>3268</td>
<td>TCP</td>
<td>Global Catalog. Active Directory integration.</td>
</tr>
<tr>
<td>3269</td>
<td>TCP</td>
<td>Secure Global Catalog. Active Directory integration.</td>
</tr>
<tr>
<td>3333</td>
<td>TCP</td>
<td>RealPresence Resource Manager or RealPresence Platform Director licensing</td>
</tr>
<tr>
<td>5060</td>
<td>TCP/UDP</td>
<td>Unencrypted SIP.</td>
</tr>
<tr>
<td>5061</td>
<td>TCP</td>
<td>SIP TLS. RealPresence Access Director communication.</td>
</tr>
<tr>
<td>5070</td>
<td>TCP</td>
<td>SIP. RealPresence Access Director communication.</td>
</tr>
<tr>
<td>5071</td>
<td>TCP</td>
<td>SIP TLS. RealPresence Access Director communication.</td>
</tr>
<tr>
<td>8443</td>
<td>TCP</td>
<td>HTTPS. RealPresence Resource Manager or RealPresence Platform Director API communication.</td>
</tr>
<tr>
<td>8444</td>
<td>TCP</td>
<td>Supercluster communication.</td>
</tr>
<tr>
<td>Port</td>
<td>Protocol</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>----------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>8989</td>
<td>TCP</td>
<td>Supercluster communication.</td>
</tr>
<tr>
<td>9333</td>
<td>TCP</td>
<td>RealPresence Resource Manager or RealPresence Platform Director licensing</td>
</tr>
</tbody>
</table>
Initial System Configuration

This section describes the configuration tasks required to complete your implementation of a new Polycom® RealPresence® DMA® system once installation and initial network configuration are complete.

This section assumes you’ve completed the configuration procedures in the Getting Started Guide (available at support.polycom.com), logged in to the Polycom RealPresence DMA system’s management interface, and verified that the Supercluster Status pane of the Dashboard shows two servers in the cluster (for a two-server configuration), with enterprise and private network status for both.

The following topics outline the configuration tasks that are generally required. If you want to complete other optional configuration tasks, refer to the appropriate section in the documentation or online help.

- DNS Records for the Polycom RealPresence DMA System
- License the Polycom RealPresence DMA System
- Set Up Signaling
- Configure the Call Server and Optionally Create a Supercluster
- Set Up Security
- Set Up MCUs
- Connect to Microsoft Active Directory®
- Set Up Conference Templates
- Test the System

DNS Records for the Polycom RealPresence DMA System

The Polycom RealPresence DMA system uses various DNS resource records configured on your DNS server(s). Some of the DNS records are required, while others may be optional.

Note: If you are not familiar with DNS administration, the creation of various kinds of DNS resource records (A/AAAA,NAPTR, NS, and SRV), your enterprise’s DNS implementation, and tuning for load balancing (if needed), please consult with someone who is.

The Polycom RealPresence DMA system requires the following records on your DNS server:

- A and/or AAAA records for IPv4 and IPv6
- The corresponding PTR records for the A and/or AAAA records

The DNS server(s) should also have entries for your Microsoft® Active Directory® server (if different from the DNS server) and any external gatekeepers or SIP peers.
You may need to create additional DNS records for SIP proxy, H.323 gatekeeper, and embedded DNS servers.

For more information about DNS, DNS records, and how DNS works, see Microsoft Technet (http://technet.microsoft.com/en-us/library/cc772774(WS.10).aspx).

**Add Required DNS Records for the Polycom RealPresence DMA System**

Your Polycom RealPresence DMA system must be accessible by its host name(s), not just its IP address(es), so you (or your DNS administrator) must create A and/or AAAA records for IPv4 and IPv6, respectively, as well as the corresponding PTR records, on your DNS server(s).

A/AAAA records and PTR records that map each physical host name to the corresponding physical IP address and each virtual host name to the corresponding virtual IP address are mandatory, as are the corresponding PTR records that allow reverse DNS resolution of the system’s physical or virtual host name(s).

*Note:* Depending on local DNS configuration, a host name could be the Polycom RealPresence DMA system’s fully qualified domain name (FQDN) or a shorter name that DNS can resolve. For some features, such as Microsoft Exchange Server integration, it is imperative that the FQDN can be resolved in DNS, especially by the Exchange server.

**Add DNS Records for SIP Proxy**

To support the use of your Polycom RealPresence DMA system as a SIP proxy server and ease future network administrative burdens, create the following DNS records (for each cluster in a supercluster, if applicable):

- SRV records for each transport protocol that identify the host names of the SIP proxies that service a particular domain. Configure these statically to point to the host names of the Call Servers in the domain. Here are example records for two clusters:
  
  _sips._tcp.example.com. 86400 IN SRV 10 1001 5061 dma-asia.example.com.
  _sips._tcp.example.com. 86400 IN SRV 10 1002 5061 dma-europe.example.com.
  _sip._tcp.example.com. 86400 IN SRV 20 1002 5060 dma-europe.example.com.
  _sip._udp.example.com. 86400 IN SRV 30 1001 5060 dma-asia.example.com.
  _sip._udp.example.com. 86400 IN SRV 30 1002 5060 dma-europe.example.com.

- Optionally, NAPTR records that describe the transport protocols supported by the SIP proxies at a domain and identify the preferred protocol. Configure these statically to match the system’s SIP transport protocol configuration.

To enable access from the public internet, create corresponding SRV records, visible from outside the firewall, for the public address of each SIP session border controller (SBC).

For more information about the use of DNS in SIP, refer to RFCs 3263 and 2782.


**Add DNS Records for the H.323 Gatekeeper**

To support the use of your Polycom RealPresence DMA system as an H.323 gatekeeper and ease future network administrative burdens, create SRV records that identify the host names of the gatekeepers that service a particular domain. These records are necessary in order to enable the optional inbound URL dialing feature. Configure them statically to point to the host names of the Call Servers in the domain. Here are example records for two clusters:

```
_h323ls._udp.example.com. 86400 IN SRV 0 1 1719 dma-asia.example.com.
_h323ls._udp.example.com. 86400 IN SRV 0 1 1719 dma-europe.example.com.
_h323cs._tcp.example.com. 86400 IN SRV 0 1 1720 dma-asia.example.com.
_h323cs._tcp.example.com. 86400 IN SRV 0 1 1720 dma-europe.example.com.
```

To enable access from the public Internet, create corresponding SRV records, visible from outside the firewall, for the public address of each H.323 session border controller (SBC).

For more information about the use of DNS in H.323, refer to the H.323 specification, Annex O, and the H.225.0 specification, Appendix IV.

**Add DNS Records for the Embedded DNS Server**

To support DNS publishing by your Polycom RealPresence DMA system’s embedded DNS servers (see Embedded DNS), a DNS NS record is needed for the physical host name of each server in each cluster in the supercluster. These records identify the Polycom RealPresence DMA system’s embedded DNS servers as authoritative for the specified logical host name. The logical host name you specify is the one in the Call server sub-domain controlled by RealPresence DMA field on the Embedded DNS page. The following example records are for two dual-server clusters:

```
callservers.example.com. 86400 IN NS dma-asia-server1.example.com.
callservers.example.com. 86400 IN NS dma-asia-server2.example.com.
callservers.example.com. 86400 IN NS dma-asia-server1.example.com.
callservers.example.com. 86400 IN NS dma-europe-server2.example.com.
```

**Note:** Do not create NS records for virtual host names.

Your enterprise DNS must also have the zone **callservers.example.com** defined and be configured to forward requests for names in that zone to any of the clusters in the supercluster. The way you do this depends on the DNS server software being used.

Queries to the enterprise DNS for **callservers.example.com** are referred to the specified RealPresence DMA clusters. Their embedded DNS servers create and manage A records for each site in the site topology. When responsibility for a site moves from one cluster to another, the A records are updated so that the site’s domain name is mapped to the new cluster.
Verify That DNS Is Working for All Addresses

To confirm that DNS can resolve all the host names and/or FQDNs, you must ping each of them, either from a command prompt on the PC you are using to access the system or from one of the clusters you are setting up.

To ping host names and FQDNs from the management interface:

1. Go to Admin > Troubleshooting Utilities > Ping.
2. In IP address or host name, enter a host name or FQDN.
3. Click Ping to confirm that DNS can resolve the host name or FQDN that you entered.

If you have access to a Linux PC and are familiar with the dig command, you can use it to query the enterprise DNS server to verify that all of the records (A/AAAA, NS, and SRV) are present and accurate.

License the Polycom RealPresence DMA System

A Polycom RealPresence DMA system's license specifies the maximum number of concurrent calls that can touch the system.

In a supercluster configuration, note the following:

- A single call may touch more than one system. The call consumes a license on each system it touches.
- Each system may be licensed for a different number of calls.
- If your superclustering strategy calls for a system to be primary for one territory and backup for another, it must be licensed for the call volume expected if it has to take over the territory for the primary system.
- License pooling is available across a supercluster or High Availability pair. Any system can share all licenses on all servers in all clusters.

The licensing process depends on the type of license you have for your product. Within the management user interface, you can enable licensing with activation keys or you can specify a licensing server.

- If you are a Polycom RealPresence Clariti™ customer with a Polycom RealPresence Resource Manager system version 10.0 or later, you must use the RealPresence Resource Manager system to license your product. If you have not deployed a RealPresence Resource Manager system or if you have not upgraded your RealPresence Resource Manager system to version 10.0 or later, you must license your product using the RealPresence Platform Director system version 3.0 or later.
- If you are not a RealPresence Clariti customer, you must use a license file to obtain an activation key code to license your product.

Set Up Signaling

Signaling setup includes configuring the following options:

- Enable H.323 signaling so that the Polycom RealPresence DMA system’s call server operates as a gatekeeper. Configuration may include these steps:
  ➢ Enable gatekeeper discovery via H.323 multicast.
Enable and configure H.235 device authentication.

- Enable SIP signaling so that the Polycom RealPresence DMA system’s call server operates as a SIP registrar and proxy server. Configuration may include these steps:
  - Configure whether to support unencrypted SIP and whether to require mutual authentication (validation of client certificates).
  - Enable pass-through of ANAT signaling (RFC 4091 and RFC 4092).
  - Enable and configure SIP digest authentication.
  - Enable and configure special handling for untrusted (“unauthorized” or “guest”) calls from SIP session border controllers (SBCs).
- Enable WebRTC signaling.

To set up signaling, follow the procedure in Set Up Signaling.

**Configure the Call Server and Optionally Create a Supercluster**

You can configure the Polycom RealPresence DMA system’s call server function and also create a supercluster if needed.

**To configure the call server and optionally create a supercluster:**

1. Integrate with a Polycom RealPresence Resource Manager system (see RealPresence Resource Manager Integration) or enter site topology information (see Site Topology).
2. If deploying a supercluster of multiple geographically distributed RealPresence DMA clusters:
   a. Set the security options in Security Settings before superclustering (see Security Settings), but wait until after superclustering to complete the remaining security setup tasks.
   b. Depending on security settings, you may need to install certificates before superclustering (see Security Certificates).
   c. Create a supercluster (see Superclustering) and configure supercluster options.
3. Create territories and assign sites to them (if you integrated with a Polycom RealPresence Resource Manager system, this must be done on that system).
4. Assign the primary and backup cluster responsible for each territory, and designate which territories can host conference rooms (see Territories).
5. Add any external devices, such as a neighbor gatekeeper or SIP peer (see External H.323 Gatekeepers, External SIP Peers, and External H.323 Session Border Controllers).
6. Configure the dial plan (see Dial Plans).

**Set Up Security**

The first step in securing your Polycom RealPresence DMA system is to locate it in a secure data center with controlled access. Then configure the security settings for your system.

Some of these steps assume you are integrating with Active Directory and some overlap with other initial setup topics.
To secure your RealPresence DMA system:

1. As the default local administrative user (admin), create a local user account for yourself with the Administrator role, log in using that account, and delete the admin user account. See Managing Users.

2. Create the Active Directory service account (read-only user account) that the Polycom RealPresence DMA system will use to read and integrate with Active Directory. See Microsoft® Active Directory® Integration.

3. Assign the Administrator role to your named enterprise account, and remove the Polycom RealPresence DMA system's user roles (see User Roles and Access Privileges) from the service account used to integrate with Active Directory. See Microsoft® Active Directory® Integration.

4. Log out and log back in using your enterprise user ID and password.

5. Verify that the expected enterprise users are available in the Polycom RealPresence DMA system and that conference room IDs were successfully created for them. If necessary, adjust integration settings and correct errors. See Microsoft® Active Directory® Integration, and Managing Users.

6. Obtain and install a security certificate from a trusted certificate authority. See Security Certificates.

7. Configure as needed various login policy settings (see Login Policy Settings) and optionally, a management access whitelist (see Management Access Settings).

8. Document your current configuration for comparison in the future. We recommend saving screen captures of all the configuration pages.

9. Manually create a backup, download it, and store it in a safe place. See Upgrading the Software.

Set Up MCUs

The Polycom RealPresence DMA system can interact with MCUs, or media servers, in either or both of the following two ways:

- MCUs may be made available to the RealPresence DMA system's conference manager to manage for multi-point conferencing (hosting virtual meeting rooms, or VMRs).
- MCUs may be registered with the RealPresence DMA system's call server as standalone MCUs and/or gateways.

This configuration summary assumes you want to do both.

- Ensure that your MCUs are configured to accept encrypted (HTTPS) management connections (required for maximum or high security mode).
- Ensure that each MCU is in a site belonging to a territory for which the Polycom RealPresence DMA system is responsible. If you’re deploying a supercluster (see Superclustering), make sure that each territory has a primary and backup cluster assigned to it. If the primary cluster becomes unavailable, the MCUs registered to it can re-register to the backup.
- If you are deploying a supercluster, verify that you’ve enabled the hosting of conference rooms in the right territories and assigned clusters to those territories. See Superclustering.
- Standalone MCUs can register themselves to the RealPresence DMA system’s Call Server. To make an MCU available as a conferencing resource, either add it to the appropriate Polycom RealPresence DMA cluster’s Conference Manager manually or, if it is already registered with the Call Server, edit its entry to enable it for conference rooms and provide the additional configuration information required. See MCU Management.
Initial System Configuration

- You must organize MCUs configured as conferencing resources into one or more MCU pools (logical groupings of media servers). Then, you can define one or more MCU pool orders that specify the order of preference in which MCU pools are used.

  Note: If you have a Polycom RealPresence Resource Manager system that’s going to use the RealPresence DMA system API to schedule conferences on the RealPresence DMA system’s conferencing resources (MCU pools), you must create MCU pools and pool orders specifically for the use of the RealPresence Resource Manager system. The pool orders should be named in such a way that:
  - They appear at the top of the pool order list presented in the RealPresence Resource Manager system.
  - Users of that system will understand that they should choose one of those pool orders.

  When adding an MCU for use by a RealPresence Resource Manager system, the option Enable for conference rooms should not be selected in the settings dialog for that MCU.

- Every conference room (VMR) is associated with an MCU pool order. The pool(s) to which an MCU belongs, and the pool order(s) to which a pool belongs, are used to determine which MCU is used to host a conference. See MCU Pools and Pool Orders for information about how to use pools and pool orders, as well as the rules that the system uses to choose an MCU for a user.

  The Polycom RealPresence DMA system uses conference templates to define the conferencing experience associated with a conference room or enterprise group. You can create standalone templates (recommended), setting the conferencing parameters directly in the Polycom RealPresence DMA system, or link templates to RealPresence® Collaboration Server or RMX MCU conference profiles (see Conference Templates).

  If you want to create RealPresence DMA system templates linked to conference profiles on the RealPresence Collaboration Server or RMX MCUs, make sure the profiles used by the Polycom RealPresence DMA system exist on all the MCUs and are defined the same on all of them.

Connect to Microsoft Active Directory®

Connecting to Microsoft® Active Directory® simplifies the task of deploying conferencing to a large organization. All Polycom RealPresence DMA system access to the Active Directory server is read-only and minimally impacts the directory performance. See Microsoft® Active Directory® Integration.

  Note: If you are not knowledgeable about enterprise directories in general and your specific implementation in particular, please consult with someone who is. Active Directory integration is a non-trivial matter.

  Active Directory integration automatically makes the enterprise users (directory members) Conferencing Users in the Polycom RealPresence DMA system, and can assign each of them a conference room (virtual meeting room, or VMR). The conference room IDs are typically generated from the enterprise users’ phone numbers.

  Note: Creating conference rooms for enterprise users is optional. If you want to integrate with Active Directory to load user and group information into the Polycom RealPresence DMA system, but do not want to give all users the ability to host conferences, you can do so. You can manually add conference rooms for selected users at any time. See Conference Rooms.
You can assign Polycom RealPresence DMA system roles to an enterprise group, applying the roles to all members of the group and enabling them to log into the Polycom RealPresence DMA system's management interface with their standard network user names and passwords.

Enterprise groups can have their own conference templates that provide a custom conferencing experience (see Conference Templates). They can also have their own MCU pool order, which preferentially routes conferences to certain MCUs (see MCU Pools and Pool Orders).

Before integrating with Active Directory, be sure that one or more DNS servers are specified (this should have been done during installation and initial setup). See Network Settings.

If you are deploying a supercluster of multiple geographically distributed Polycom RealPresence DMA clusters, verify that you have assigned clusters to the territories in your site topology (see Superclustering) and decide which cluster is to be responsible for Active Directory integration.

Once the Polycom RealPresence DMA system is integrated with Active Directory, it reads the directory information nightly, so that user and group information is updated automatically as people join and leave the organization. The system caches certain data from Active Directory. In a superclustered system, one cluster is responsible for updating the cache, which is shared with all the clusters.

Between updates, clusters access the directory only to authenticate passwords (for instance, for the management interface login); all other user information (such as user search results) comes from the cache. You can manually update the cache at any time.

See Managing Users, Groups, and Working with Enterprise Groups.

There are security concerns that need to be addressed regarding user accounts, whether local or enterprise. See Security Settings.

Set Up Conference Templates

The Polycom RealPresence DMA system uses conference templates and global conference settings to manage system and conference behavior, and it has a default conference template and default global conference settings.

Templates allow you to specify most conference parameters:

- General information such as line rate, encryption, auto termination, and H.239 settings
- Video settings such as mode (presentation or lecture) and layout
- IVR settings
- Conference recording settings

After you have added MCUs to the system, you may want to change the global conference settings or create additional templates that specify different conference properties.

If you integrate with Active Directory, you can use templates to provide customized conferencing experiences for various enterprise groups.

When you add a custom conference room to a user (either local or enterprise), you can choose which template that conference room uses.

To add conference templates, see Conference Templates. To change conference settings, see Conference Settings. To customize the conferencing experience for an enterprise group, see Working with Enterprise Groups.
Test the System

You can test your Polycom RealPresence DMA system in various ways.

1. On the Sip Settings and H.323 Settings pages, verify that:
   - If you enabled H.323, the Status field in the H.323 Settings section indicates that the signaling status is Active and the port assignments are correct.
   - If you enabled SIP, the SIP Settings section shows that the correct protocols and listening ports are enabled.

2. Have some endpoints register with the RealPresence DMA system and make point-to-point calls to each other.

3. On the Dashboard, verify that:
   - The information in the Cluster Info pane looks correct, including the time, network settings, and system resource information.
   - The Supercluster Status pane shows the correct number of servers and clusters, and the network interfaces that should be working (depending on your IP type and split network settings) are up (green up arrow) and in full duplex mode, with the speed correct for your enterprise network.
   - The Call Server Registrations pane shows that the endpoints that attempted to register did so successfully.
   - The Call Server Active Calls pane shows that the endpoints that made calls did so successfully, and the call limits per cluster and total are correct for your licenses.
   - The Conference Manager MCUs pane shows that the MCUs you added are connected and in service.
   - The information on the Active Directory Integration pane looks correct, including the status, cache refresh data, and enterprise conference room count.

4. Set up some multipoint conferences by having endpoints dial into enterprise users’ conference rooms (preferably including a custom conference room). Verify that conferencing works satisfactorily, that the system status is good, and that the Conference Manager Usage pane accurately presents the status.

When you’re satisfied that the Polycom RealPresence DMA system is configured and working properly, manually create a backup, download it, and store it in a safe place. See Backing Up and Restoring.
Server Configuration

This section provides an introduction to the Polycom® RealPresence® DMA® system configuration. It includes:

- Network Settings
- Signaling Settings
- High Availability Settings
- Configure Time Settings
- Configure Alert Settings
- Configure Logging Settings
- Licenses
- Security Settings
- Security Certificates
- Usage Data
Server Settings

Some of the following Polycom® RealPresence® DMA® system settings can be configured during system installation. Any of the settings can be revised as needed.

- Network Settings
- Configure Time Settings
- Configure Logging Settings
- Configure Alert Settings
- Changing the Linux Root Password
- Usage Data

If you are performing the initial configuration of your Polycom RealPresence DMA system, refer to Initial System Configuration before you continue.

Network Settings

Some of the General System Network Settings are configured during system installation and rarely need to be changed. Revising some network settings (host names, IP addresses, or domains) requires a system restart and terminates all active conferences.

If the RealPresence DMA system is using a CA-provided identity certificate, changing some network settings (host names or IP addresses) also requires you to update the certificate. If the revised settings require a new certificate, the system will automatically generate a new self-signed certificate.

You cannot configure or revise network settings under the following circumstances:

- While the system is part of a supercluster – you must first leave the supercluster and, if the cluster is responsible for any territories (as primary or backup), reassign those territories. After the change, rejoin the supercluster.
- When the system is integrated with a Polycom RealPresence Resource Manager system – you must first terminate the integration. After the change, reintegrate with the Polycom RealPresence Resource Manager system.
- When the system is configured for High Availability (HA) – you must disable HA before you revise any network settings.

Configure General System Network Settings

Some of the General System Network Settings are configured during system installation but can be changed when necessary. Note that changing some network settings (host names, IP addresses, or domains) requires a system restart and terminates all active conferences.
To configure general network settings:

1. Go to Admin > Server > Network Settings.
2. Complete the fields described in the following table as required.

### General System Network Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General System Network Settings</strong></td>
<td>The settings in this section apply to the entire system and aren’t specific to management or signaling.</td>
</tr>
<tr>
<td>System IP type</td>
<td>Displays which address families are currently enabled (IPv4 or IPv6). Use the Actions menu to enable or disable an address family.</td>
</tr>
<tr>
<td>Host name</td>
<td>The host name of the system. If a DHCP server assigned the host name during system installation, you can select Override DHCP Settings and enter a host name that overrides the DHCP-assigned host name.</td>
</tr>
<tr>
<td>Domain</td>
<td>The domain for the system. This is combined with the host name to form the fully qualified domain name (FQDN). For instance:</td>
</tr>
</tbody>
</table>
|                              | Host name: dma1
|                              | Domain: callservers.example.com
|                              | FQDN: dma1.callservers.example.com
|                              | If a DHCP server assigned the domain during system installation, you can select Override DHCP Settings and enter a domain that overrides the DHCP-assigned domain. |
| DNS search domains           | One or more fully qualified domain names, separated by commas or spaces. The domain you enter for the system is added automatically.        |
|                              | If a DHCP server assigned DNS search domains during system installation, you can select Override DHCP Settings and enter DNS search domains that override the ones assigned by DHCP. |
| DNS 1                        | IP addresses of up to three domain name servers. At least one DNS server is required.                                                         |
| DNS 2                        | DNS queries on any configured network interface will be sent to the same DNS name servers (in order).                                      |
| DNS 3                        | If a DHCP server assigned DNS 1 during system installation, you can select Override DHCP Settings and enter a primary DNS that overrides the one assigned by DHCP. |
|                              | Note that the system only uses the secondary DNS server if the primary DNS server is unreachable, and only uses the tertiary DNS server if the primary and secondary servers are unreachable. |
|                              | Your RealPresence DMA system must be accessible by its host name(s), not just its IP address(es), so you (or your DNS administrator) must create A and/or AAAA records for IPv4 and IPv6, respectively, as well as the corresponding PTR records, on your DNS server(s). A/AAAA records and PTR records that map each physical host name to the corresponding physical IP address and each virtual host name to the corresponding virtual IP address are mandatory, as are the corresponding PTR records that allow reverse DNS resolution of the system’s physical or virtual host name(s). |
Configure Network Interface Settings

You can configure general, IPv4, and IPv6 settings for any network interface. Note that Link Settings and LAN Security Settings can be configured only for NIC interfaces.

To configure network interface settings:

1. Go to Admin > Server > Network Settings.
2. In the Network Interface Settings section, select an interface to configure and click Edit Selected Interface.
3. Configure the settings for the network interface as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of a NIC network interface is not editable. The names of bonded and VLAN interfaces are generated.</td>
</tr>
<tr>
<td>MAC address</td>
<td>The MAC address of the network interface card.</td>
</tr>
<tr>
<td>Enabled</td>
<td>If an interface has services assigned to it, it cannot be disabled. Services must first be re-assigned to another interface.</td>
</tr>
</tbody>
</table>

**IP Configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 boot protocol</td>
<td>The IPv4 boot protocol of the network interface. Options are STATIC or DHCP.</td>
</tr>
<tr>
<td>IPv4 address/prefix length*</td>
<td>IPv4 address and the CIDR (Classless Inter-Domain Routing) prefix size of the interface.</td>
</tr>
<tr>
<td>IPv4 gateway*</td>
<td>IPv4 address of the gateway server used to route network traffic outside the subnet.</td>
</tr>
<tr>
<td>IPv6 boot protocol</td>
<td>The IPv6 boot protocol of the network interface. Options are STATIC, SLAAC, or DHCP.</td>
</tr>
<tr>
<td>IPv6 (global) address/prefix length</td>
<td>IPv6 address and the CIDR (Classless Inter-Domain Routing) prefix size value (the number of leading 1 bits in the routing prefix mask) that defines the subnetwork of the system’s management or combined interface.</td>
</tr>
<tr>
<td>IPv6 (link-local)</td>
<td>The IPv6 link-local address, which is not visible outside of the link.</td>
</tr>
<tr>
<td>IPv6 gateway</td>
<td>IPv6 address of the gateway server used to route network traffic outside the local link.</td>
</tr>
</tbody>
</table>

**Link Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-negotiation</td>
<td>Turn on Auto-negotiation or set Speed and Duplex manually.</td>
</tr>
<tr>
<td>Speed</td>
<td>Note: Auto-negotiation is required if your network is 1000Base-T. Do not select 10000 unless you are certain your hardware platform supports it.</td>
</tr>
<tr>
<td>Duplex</td>
<td></td>
</tr>
</tbody>
</table>
Configure Service Settings

You can assign RealPresence DMA system signaling and management services to any interface that is enabled and configured either statically or dynamically with IP addresses. The services (signaling, management) can be assigned to the same or different interfaces. Note that interfaces without services assigned may still be used in High Availability (HA) configurations for HA communication between systems.

To configure service settings:

1. Go to Admin > Server > Network Settings.
2. In the ACTIONS section, click Service Settings.
3. Configure the signaling and management settings as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signaling Settings</td>
<td></td>
</tr>
<tr>
<td>Signaling interface</td>
<td>The interface the RealPresence DMA system uses for signaling traffic. This may be a network interface card, a VLAN interface, or a bonded interface.</td>
</tr>
<tr>
<td>Signaling DSCP</td>
<td>The Differentiated Services Code Point value (0 - 63) to put in the DS field of IP packet headers on outbound packets associated with signaling traffic. The DSCP value is used to classify packets for quality of service (QoS) purposes. If you are not sure what value to use, leave the default of 0.</td>
</tr>
</tbody>
</table>
Routing Configuration

If your network configuration requires specific routing for some subnet(s), you can use static routes to handle the requirements.

Add a Static Route

You can only configure static route settings that are valid for the current network settings. If you need to change both the network settings and routing configuration, change the network settings first to prevent system errors.

To add a static route:

1. Go to Admin > Server > Network Settings.
2. Under Actions, click Routing Configuration.
3. Select the Default gateway device.
   - The Default gateway device is the network interface designated as the default route when no other routing rules match the destination network address.
4. Click Add Route.
5. Complete the fields in the following table as required:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Select the interface for this route.</td>
</tr>
<tr>
<td>Subnet</td>
<td>The target address prefix for the route. It should consist of a network specification, e.g., &quot;192.168.9.0&quot; or &quot;192.168.0.0&quot;.</td>
</tr>
<tr>
<td>Prefix length</td>
<td>The CIDR (Classless Inter-Domain Routing) prefix size value (the number of leading 1 bits in the routing prefix mask). This value, together with the Subnet address, define the destination network for this route.</td>
</tr>
<tr>
<td>Via</td>
<td>IP address of the next hop or gateway for this route.</td>
</tr>
</tbody>
</table>
6 Click OK.
   The static route displays in the Static Routes table.
7 Repeat the preceding steps to add more routes.
8 When you have added all necessary routes, click OK.

Delete a Static Route
You can delete static routes as needed.

To delete a static route:
1 Go to Admin > Server > Network Settings.
2 Under Actions, click Routing Configuration.
3 Select a static route from the list and click Delete Selected Route to delete it.
4 Click OK.

Bonded and VLAN Interfaces
The RealPresence DMA system supports the use of logical interfaces in addition to physical network interfaces. You can add bonded and VLAN interfaces that can provide increased bandwidth and redundancy capabilities for your network interfaces.

A bonded interface can be configured to combine two or more physical NICs into a single logical network interface. This is also known as Link Aggregation. When bonded, the NICs appear to be the same physical device. Bonding requires a switch that supports and is configured for Link Aggregation Control protocol (LACP), as described in IEEE 802.3ad.

VLAN interfaces can be created by splitting a single NIC link into multiple logical links. The physical NIC defines the VLAN interfaces (e.g., eth1.1, eth1.2, etc.), each of which is a logical network interface configured with an IP address. Each VLAN interface is associated with a subnet on a VLAN trunk supplied by a switch that carries VLAN traffic, as described in IEEE 802.1Q. An aggregated link (bonded interface) can also be configured to deliver a VLAN trunk.

You can assign RealPresence DMA system services such as management and signaling to both physical and logical interfaces. Also, both types of interfaces can be used for communication between two RealPresence DMA systems configured for High Availability.

Note that the NICs associated with a logical interface should not be:
   ● Assigned IP addresses
   ● Used in firewall rules
   ● Used in network packet captures
   ● Used in traceroute
   ● Used in ping

Add a Bonded Interface
A bonded interface can increase available bandwidth and provide NIC failover protection. You can add a bonded interface to combine two or more NICs into a single logical network connection. The logical network
interface is typically represented by bond0, bond1...bondn. The NICs (eth1, eth2, etc.) are considered slaves of the bonded interface.

To add a bonded interface:

1. Go to Admin > Server > Network Settings.
2. Under ACTIONS, click Add Bonded Interface.
3. Configure the settings for the bonded interface as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Bonded</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>The RealPresence DMA system generates the name of the interface based on the number of bonded interfaces already configured, starting with bond0 and incrementing by 1, e.g., bond1, bond2, etc.</td>
</tr>
<tr>
<td>Enable</td>
<td>Select the check box if the bonded interface will be assigned IP addresses. If the bonded interface is configured at the switch to deliver a VLAN trunk, complete the necessary configuration and then uncheck the Enable check box before clicking OK to save the interface. You will add one or more VLAN interfaces later, which will automatically enable the bonded interface.</td>
</tr>
<tr>
<td>Available NICs</td>
<td>The interfaces available for aggregation.</td>
</tr>
<tr>
<td>Bonding policy</td>
<td>This policy is applied to the bonded interface but the switch must be configured to support the policy you select. The following bonding policy values are available:</td>
</tr>
<tr>
<td></td>
<td>balance-rr – Sets a round-robin policy for fault tolerance and load balancing. Transmissions are received and sent out sequentially on each bonded slave interface beginning with the first one available.</td>
</tr>
<tr>
<td></td>
<td>active-backup – Sets an active-backup policy for fault tolerance. Transmissions are received and sent out via the first available bonded slave interface. Another bonded slave interface is only used if the active bonded slave interface fails.</td>
</tr>
<tr>
<td></td>
<td>balance-xor – Sets an XOR (exclusive-or) policy for fault tolerance and load balancing. Using this method, the interface matches the incoming request's MAC address with the MAC address for one of the slave NICs. Once this link is established, transmissions are sent out sequentially beginning with the first available interface.</td>
</tr>
<tr>
<td></td>
<td>broadcast – Sets a broadcast policy for fault tolerance. All transmissions are sent on all slave interfaces.</td>
</tr>
<tr>
<td></td>
<td>802.3ad – Sets an IEEE 802.3ad dynamic link aggregation policy. Creates aggregation groups that share the same speed and duplex settings. Transmits and receives on all slaves in the active aggregator. Requires a switch that is 802.3ad compliant.</td>
</tr>
</tbody>
</table>
### Server Settings

**Field** | **Description**
---|---
**balance-tlb** – Sets a Transmit Load Balancing (TLB) policy for fault tolerance and load balancing. The outgoing traffic is distributed according to the current load on each slave interface. Incoming traffic is received by the current slave. If the receiving slave fails, another slave takes over the MAC address of the failed slave. This mode is only suitable for local addresses known to the kernel bonding module and therefore cannot be used behind a bridge with virtual machines.  
**balance-alb** – Sets an Adaptive Load Balancing (ALB) policy for fault tolerance and load balancing. Includes transmit and receive load balancing for IPv4 traffic. Receive load balancing is achieved through ARP negotiation. This mode is only suitable for local addresses known to the kernel bonding module and therefore cannot be used behind a bridge with virtual machines.

**Link monitoring** | When selected, enables the RealPresence DMA system to monitor the physical NICs to ensure they are working. Primarily used for bonding policies that provide redundancy.

**Monitoring frequency (ms)** | If **Link monitoring** is selected, specify how often the system checks the physical NICs. A recommended starting point is 100 ms.

**Link up delay (ms)** | The length of time the system waits before enabling a link connection after a restart; must be a multiple of the **Monitoring frequency** value. Entering zero disables the link up delay.

**Link down delay (ms)** | The length of time the system waits after a link fails before disabling the connection; must be a multiple of the **Monitoring frequency** value. Entering zero disables the link down delay.

### IPv4 Configuration

**IPv4 boot protocol** | The IPv4 boot protocol of the network interface. Options are **STATIC** or **DHCP**.

**IPv4 address/prefix length** | IPv4 address and CIDR (network mask) that defines the subnetwork of the system’s management or combined interface.

**IPv4 gateway** | IPv4 address of the gateway server used to route network traffic outside the subnet.

### IPv6 Configuration

**IPv6 boot protocol** | The IPv6 boot protocol of the network interface. Options are **STATIC**, **SLAAC**, or **DHCP**.

**IPv6 (global) address/prefix length** | IPv6 address and the CIDR (Classless Inter-Domain Routing) prefix size value (the number of leading 1 bits in the routing prefix mask) that defines the subnetwork of the system’s management or combined interface.

**IPv6 (link-local)** | The IPv6 link-local address, which is not visible outside of the link.

**IPv6 gateway** | IPv6 address of the gateway server used to route network traffic outside the subnet.

4. Click **OK**.
Edit a Bonded Interface

You can edit the network interface settings for a bonded interface when necessary. A bonded interface can increase available bandwidth and provide NIC failover protection. You can add a bonded interface to combine two or more NICs into a single logical network connection. The logical network interface is typically represented by bond0, bond1...bondn. The NICs (eth1, eth2, etc.) are considered slaves of the bonded interface.

To edit a bonded interface:

1. Go to Admin > Server > Network Settings.
2. Under Network Interface Settings, select the bonded interface to edit.
3. Click the Edit button at the top of the table.
4. Configure the settings for the bonded interface as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Bonded</td>
<td>The RealPresence DMA system generates the name of the interface based on the number of bonded interfaces already configured, starting with bond0 and incrementing by 1, e.g., bond1, bond2, etc.</td>
</tr>
<tr>
<td>Name</td>
<td>Select the check box if the bonded interface will be assigned IP addresses. If the bonded interface is configured at the switch to deliver a VLAN trunk, complete the necessary configuration and then uncheck the Enable check box before clicking OK to save the interface. You will add one or more VLAN interfaces later, which will automatically enable the bonded interface.</td>
</tr>
<tr>
<td>Available NICs</td>
<td>The interfaces available for aggregation.</td>
</tr>
<tr>
<td>Bonding policy</td>
<td>This policy is applied to the bonded interface but the switch must be configured to support the policy you select.  The following bonding policy values are available:  <strong>balance-rr</strong> – Sets a round-robin policy for fault tolerance and load balancing. Transmissions are received and sent out sequentially on each bonded slave interface beginning with the first one available.  <strong>active-backup</strong> – Sets an active-backup policy for fault tolerance. Transmissions are received and sent out via the first available bonded slave interface. Another bonded slave interface is only used if the active bonded slave interface fails.  <strong>balance-xor</strong> – Sets an XOR (exclusive-or) policy for fault tolerance and load balancing. Using this method, the interface matches the incoming request's MAC address with the MAC address for one of the slave NICs. Once this link is established, transmissions are sent out sequentially beginning with the first available interface.  <strong>broadcast</strong> – Sets a broadcast policy for fault tolerance. All transmissions are sent on all slave interfaces.  <strong>802.3ad</strong> – Sets an IEEE 802.3ad dynamic link aggregation policy. Creates aggregation groups that share the same speed and duplex settings. Transmits and receives on all slaves in the active aggregator. Requires a switch that is 802.3ad compliant.</td>
</tr>
</tbody>
</table>
### Server Settings

**balance-tlb** – Sets a Transmit Load Balancing (TLB) policy for fault tolerance and load balancing. The outgoing traffic is distributed according to the current load on each slave interface. Incoming traffic is received by the current slave. If the receiving slave fails, another slave takes over the MAC address of the failed slave. This mode is only suitable for local addresses known to the kernel bonding module and therefore cannot be used behind a bridge with virtual machines.

**balance-alb** – Sets an Adaptive Load Balancing (ALB) policy for fault tolerance and load balancing. Includes transmit and receive load balancing for IPv4 traffic. Receive load balancing is achieved through ARP negotiation. This mode is only suitable for local addresses known to the kernel bonding module and therefore cannot be used behind a bridge with virtual machines.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link monitoring</td>
<td>When selected, enables the RealPresence DMA system to monitor the physical NICs to ensure they are working. Primarily used for bonding policies that provide redundancy.</td>
</tr>
<tr>
<td>Monitoring frequency (ms)</td>
<td>If Link monitoring is selected, specify how often the system checks the physical NICs. A recommended starting point is 100 ms.</td>
</tr>
<tr>
<td>Link up delay (ms)</td>
<td>The length of time the system waits before enabling a link connection after a restart; must be a multiple of the Monitoring frequency value. Entering zero disables the link up delay.</td>
</tr>
<tr>
<td>Link down delay (ms)</td>
<td>The length of time the system waits after a link fails before disabling the connection; must be a multiple of the Monitoring frequency value. Entering zero disables the link down delay.</td>
</tr>
</tbody>
</table>

### IPv4 Configuration

<table>
<thead>
<tr>
<th>IPv4 boot protocol</th>
<th>The IPv4 boot protocol of the network interface. Options are <strong>STATIC</strong> or <strong>DHCP</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 address/prefix length</td>
<td>IPv4 address and CIDR (network mask) that defines the subnetwork of the system’s management or combined interface.</td>
</tr>
<tr>
<td>IPv4 gateway</td>
<td>IPv4 address of the gateway server used to route network traffic outside the subnet.</td>
</tr>
</tbody>
</table>

### IPv6 Configuration

<table>
<thead>
<tr>
<th>IPv6 boot protocol</th>
<th>The IPv6 boot protocol of the network interface. Options are <strong>STATIC</strong>, <strong>SLAAC</strong>, or <strong>DHCP</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 (global) address/prefix length</td>
<td>IPv6 address and the CIDR (Classless Inter-Domain Routing) prefix size value (the number of leading 1 bits in the routing prefix mask) that defines the subnetwork of the system’s management or combined interface.</td>
</tr>
<tr>
<td>IPv6 (link-local)</td>
<td>The IPv6 link-local address, which is not visible outside of the link.</td>
</tr>
<tr>
<td>IPv6 gateway</td>
<td>IPv6 address of the gateway server used to route network traffic outside the subnet.</td>
</tr>
</tbody>
</table>

5 Click **OK**.
Add a VLAN Interface

VLAN interfaces can be created by splitting a single NIC link into multiple logical links. The physical NIC defines the VLAN interfaces (e.g., eth1.1, eth1.2, etc.), each of which is a logical network interface configured with an IP address. Each VLAN interface is associated with a subnet on a VLAN trunk supplied by a switch that carries VLAN traffic, as described in IEEE 802.1Q. An aggregated link (bonded interface) can also be configured to deliver a VLAN trunk.

To add a VLAN interface:

1. Go to Admin > Server > Network Settings.
2. Under ACTIONS, click Add VLAN Interface.
3. Configure the settings for the VLAN interface as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The RealPresence DMA system assigns the name of the VLAN interface when you save the VLAN Interface Settings. The name is a combination of the interface (NIC or bond) on which you create the VLAN interface and the VLAN ID, for example, eth2.1, where eth2 is the parent interface and 1 is the VLAN ID.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The numeric ID of the VLAN interface. The ID specifies the individual network within the VLAN trunk that the interface will be connected to.</td>
</tr>
<tr>
<td>Interface</td>
<td>The available interfaces (NIC or bond) on which you can create a VLAN interface.</td>
</tr>
<tr>
<td>IP Configuration</td>
<td></td>
</tr>
<tr>
<td>IPv4 boot protocol</td>
<td>The IPv4 boot protocol of the network interface. Options are STATIC or DHCP.</td>
</tr>
<tr>
<td>IPv4 address/prefix length</td>
<td>IPv4 address and CIDR (network mask) that defines the subnetwork of the system's management or combined interface.</td>
</tr>
<tr>
<td>IPv4 gateway</td>
<td>IPv4 address of the gateway server used to route network traffic outside the subnet.</td>
</tr>
<tr>
<td>IPv6 boot protocol</td>
<td>The IPv6 boot protocol of the network interface. Options are STATIC, SLAAC, or DHCP.</td>
</tr>
<tr>
<td>IPv6 (global) address/prefix length</td>
<td>IPv6 address and the CIDR (Classless Inter-Domain Routing) prefix size value (the number of leading 1 bits in the routing prefix mask) that define the subnetwork of the system's management or combined interface. Routable anywherescoped globally.</td>
</tr>
<tr>
<td>IPv6 (link-local)</td>
<td>The IPv6 link-local address, which is not visible outside of the link.</td>
</tr>
<tr>
<td>IPv6 gateway</td>
<td>IPv6 address of the gateway server used to route network traffic outside the subnet.</td>
</tr>
</tbody>
</table>

4. Click OK.
Edit a VLAN Interface

VLAN interfaces can be created by splitting a single NIC link into multiple logical links. The physical NIC defines the VLAN interfaces (e.g., eth1.1, eth1.2, etc.), each of which is a logical network interface configured with an IP address. Each VLAN interface is associated with a subnet on a VLAN trunk supplied by a switch that carries VLAN traffic, as described in IEEE 802.1Q. An aggregated link (bonded interface) can also be configured to deliver a VLAN trunk.

To edit a VLAN interface:

1. Go to Admin > Server > Network Settings.
2. Under Network Interface Settings, select the VLAN interface to edit.
3. Click the Edit button at the top of the table.
4. Configure the settings for the VLAN interface as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The RealPresence DMA system assigns the name of the VLAN interface when you save the VLAN Interface Settings. The name is a combination of the interface (NIC or bond) on which you create the VLAN interface and the VLAN ID, for example, eth2.1, where eth2 is the parent interface and 1 is the VLAN ID.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The numeric ID of the VLAN interface. The ID specifies the individual network within the VLAN trunk that the interface will be connected to.</td>
</tr>
<tr>
<td>Interface</td>
<td>The available interfaces (NIC or bond) on which you can create a VLAN interface.</td>
</tr>
<tr>
<td><strong>IP Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>IPv4 boot protocol</td>
<td>The IPv4 boot protocol of the network interface. Options are STATIC or DHCP.</td>
</tr>
<tr>
<td>IPv4 address/prefix length</td>
<td>IPv4 address and CIDR (network mask) that defines the subnetwork of the system's management or combined interface.</td>
</tr>
<tr>
<td>IPv4 gateway</td>
<td>IPv4 address of the gateway server used to route network traffic outside the subnet.</td>
</tr>
<tr>
<td>IPv6 boot protocol</td>
<td>The IPv6 boot protocol of the network interface. Options are STATIC, SLAAC, or DHCP.</td>
</tr>
<tr>
<td>IPv6 (global) address/prefix length</td>
<td>IPv6 address and the CIDR (Classless Inter-Domain Routing) prefix size value (the number of leading 1 bits in the routing prefix mask) that define the subnetwork of the system's management or combined interface. Routable anywhere/scoped globally.</td>
</tr>
<tr>
<td>IPv6 (link-local)</td>
<td>The IPv6 link-local address, which is not visible outside of the link.</td>
</tr>
<tr>
<td>IPv6 gateway</td>
<td>IPv6 address of the gateway server used to route network traffic outside the subnet.</td>
</tr>
</tbody>
</table>

5. Click OK.
Enable IPv6

You can configure your RealPresence DMA network settings to use IPv4 or IPv6 addressing. However, the system also supports IPv4 and IPv6 addressing simultaneously in a mixed mode environment.

To enable IPv6 Settings:

1. Go to Admin > Server > Network Settings.
2. Click Enable IPv6.
   A list of all enabled network interfaces displays.
3. For each enabled interface, configure the following settings:
   - **Type** – the system IP address type (STATIC, DHCP6, or SLAAC)
   - **IPv6 Address**
   - **IPv6 Gateway**
4. Click OK to enable IPv6 addressing.

Enable IPv4

You can configure your RealPresence DMA network settings to use IPv4 or IPv6 addressing. However, the system also supports IPv4 and IPv6 addressing simultaneously in a mixed mode environment.

To enable IPv4 Settings:

1. Go to Admin > Server > Network Settings.
2. Click Enable IPv4.
   A list of all enabled network interfaces displays.
3. For each enabled interface, configure the following settings:
   - **Type** – the system IP address type (STATIC, DHCP6, or SLAAC)
   - **IPv4 Address**
   - **IPv4 Gateway**
4. Click OK to enable IPv4 addressing.

Configure Time Settings

For Polycom RealPresence DMA Appliance Edition systems, you can configure time settings with the USB Configuration Utility during first-time setup of your system. You can change a system’s (or cluster’s) time settings at any time, but note that this requires a system restart and terminates all active conferences.

For RealPresence DMA Virtual Edition systems, time settings are typically inherited from the RealPresence Resource Manager system or manually configured. See the Polycom® RealPresence® DMA® System Getting Started Guide.

Polycom recommends specifying at least one but preferably three NTP time servers. You must specify at least one time server before creating or joining a supercluster.
To configure time settings:

1. Go to Admin > Server > Time Settings.
2. Edit the fields in the following table as required.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System time zone</td>
<td>Time zone in which the system is located. Polycom recommends selecting the time zone of a specific geographic location (such as America/Denver), not one of the generic GMT offsets (such as GMT+07 POSIX). If you use a generic GMT offset (for instance, to prevent automatic daylight saving time adjustments), note that they use the Linux/Posix convention of specifying how many hours ahead of or behind local time GMT is. Thus, the generic equivalent of America/Denver (UTC-07:00) is GMT+07, not GMT-07.</td>
</tr>
<tr>
<td>Use NTP Server</td>
<td>Specify the IP Address or Host Name (FQDN) of up to three time servers for maintaining system time. Polycom recommends specifying at least one but preferably three NTP time servers.</td>
</tr>
<tr>
<td>Manually set system time</td>
<td>While not recommended, you can manually specify the System Date and System Time.</td>
</tr>
</tbody>
</table>

3. When finished, click Update.

Configure Logging Settings

You can configure the system's logging settings for local and forwarded logs.

To configure log settings:

1. Go to Admin > Server > Logging Settings.
2. Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging level</td>
<td>Leave the default, Debug, unless advised to change it by Polycom support. Production reduces system overhead and log file sizes, but omits information that’s useful for troubleshooting. Verbose debug is not recommended for production systems.</td>
</tr>
<tr>
<td>Rolling frequency</td>
<td>If rolling the logs daily (the default) produces logs that are too large, shorten the interval.</td>
</tr>
<tr>
<td>Maximum retention time</td>
<td>The number of days to keep log archives.</td>
</tr>
</tbody>
</table>
Configure Alert Settings

You can configure thresholds for system alerts, enable or disable certain alerts, and control when they will be triggered.

The same threshold settings are used for both system alerts and SNMP alerts.

Certificate-related alert settings cannot be modified.

To configure alert settings:

1. Go to Admin > Server > Alert Settings.

   The Alert Settings page lists the following alert settings.

2. Click Update.

3. Click OK.
To enable an alert, mark the associated check box.

3 To change the Threshold Value, make sure the associated check box is marked and then use the arrows next to each field or enter a new number to change the default value.

4 Click the Update button to save your changes.

5 To revert your changes, click Select Defaults. When you click Select Defaults, all values return to their factory defaults.

## Changing the Linux Root Password

Enterprise and local Administrators can change the Linux OS root password for the RealPresence DMA system without entering a shell interface.

In normal system operations, RealPresence DMA users, including Administrators, do not need to know or use the Linux root password. However, if the root password has been compromised or if corporate security policies require changing all system passwords at certain intervals or after specific events occur, you can change the root password.

Consider the following details before changing the Linux root password:

- Only Administrators may change the Linux root password. The menu option does not display to Auditors, Provisioners, or users without an assigned role.
You must log in to the physical address of a RealPresence DMA server to change its Linux root password:

- In a two-server cluster, you must log in to each server to change its root password.
- Although not required, Polycom recommends that the two servers have the same Linux root password.

Password complexity rules are based on the local password policy settings (see Configure Local Password Settings), with the following exceptions:

- The Linux root password does not expire.
- Previously used root passwords can be reused.

You can attempt to change the root password only once per minute.

Upgrading the RealPresence DMA system software does not change the root password.

If you restore the RealPresence DMA system from a backup file and select the IP network, certificate, security and licensing configuration system backup components, the Linux root password of the restored system will be the same as the root password of the system at the time you created the backup.

Caution: If you change the Linux root password, Polycom Global Services cannot access the operating system of your RealPresence DMA system. As a result, support services may be limited.

**Change the Linux Root Password**

You can change the Linux OS root password for the RealPresence DMA system from the management user interface.

**To change the Linux root password**

1. Go to **Admin > Server > Change Linux Root Password**.
2. Complete the password fields as follows:
   - **Old password**: If the Linux root password has not been changed since the system was installed, leave this field blank. If the Linux root password has been changed one or more times, enter the current password.
   - **New password**: Enter the new root password.
   - **Confirm new password**: Re-enter the new root password.
3. Click **OK**.

**Usage Data**

To continually improve the product, Polycom collects data to understand how customers use the RealPresence DMA system. By collecting this data, Polycom can identify system level utilization and the combined use of RealPresence DMA system features. This data informs Polycom which features are important and actually used on your system. Polycom uses this information to help guide future development and testing.

Your decision to enable or not enable the sending of this data does not affect the availability of any documented system feature in any way. Enabling this feature does not affect the capacity or responsiveness
of the RealPresence DMA system to process calls and conferences, nor does it affect access to the web user interface or API interactions.

The system sends usage data once per hour over a secured (TLS) connection (port 8443) to a Polycom collection point (customerusagedatacollection.polycom.com). There is no access by any customer or others to view the data received at the collection point. The raw data is viewable only by Polycom. To avoid any impact to starting and ending calls and conferences, data is never sent between 5 minutes before the hour and 5 minutes after the hour.

The following types of data are reported:

- License information
- Hardware configuration
- System resource usage: CPU, RAM, disk, database
- System configuration: number of servers, clusters
- Feature configuration: Enterprise Directory Integration, Skype for Business, Dial Rules, Shared Number Dialing, Hunt Groups, Registration Policy, Device Authentication
- Number of users, endpoints, sites, MCUs, external gatekeepers, SIP peers, SBCs
- Registrations, call and conference statistics
- Security settings

If you enable data collection, your user and environment identifying information (e.g., internal IP addresses and FQDNs, names of users, devices, external systems, etc.) is made anonymous before the RealPresence DMA system sends usage data to the data collection point. System serial numbers and license information are sent without anonymization and may be used to help improve customer experiences. In total, less than 100KB of data per hour is collected and sent.

Polycom’s collection and use of this data complies with Polycom’s Privacy Policy.

**Enable or Disable Automatic Data Collection**

You can allow or disallow the automatic sending of usage data when you accept the system’s End User License Agreement.

The RealPresence DMA system requires HTTPS port 8443 to be open to send usage data.

You can enable or disable this feature at any time.

**To enable or disable automatic data collection:**

1. Go to Admin > Server > Licenses.
2. Mark or unmark the Automatically send usage data check box.

**See the Collected Usage Data**

The system records data that has been sent and collected in the system logs.

**To see the collected data:**

1. Log in to the RealPresence DMA system as an Administrator.
2 Download the system logs.

3 On the PC where the logs have been downloaded, use an archiving or zipping tool to extract the file `analytics.json`.

   *Analytics.json* is a text file containing the hourly data reported most recently before the time when the system logs were created.

4 View the `analytics.json` file with Notepad or another text editing tool.
Signaling Settings

The RealPresence DMA system supports H.323, SIP, and WebRTC signaling protocols. At least one of the protocols must be enabled in order for the RealPresence DMA system’s Conference Manager to receive calls for multipoint conferences and distribute them among the MCUs configured on the system.

H.323, SIP, and WebRTC Signaling

If H.323 signaling is enabled, the Polycom RealPresence DMA system’s Call Server operates as a gatekeeper, receiving registration requests and calls from H.323 devices. If SIP signaling is enabled, the Call Server operates as a SIP registrar and proxy server, receiving registration requests and calls from SIP devices. If WebRTC signaling is enabled, the Call Server processes Polycom® RealPresence® Web Suite conferences initiated from WebRTC-capable web browsers. If you enable more than one signaling protocol, the RealPresence DMA system allows devices using different protocols to communicate in multipoint conferences.

H.323, SIP, and WebRTC signaling settings are specific to an individual cluster. When you add a cluster to a supercluster, the cluster’s signaling settings are not changed to match the settings of any other member of the supercluster. To avoid confusion, Polycom recommends that H.323, SIP, and WebRTC signaling settings be configured the same across all clusters in a supercluster, except when a specific deployment requires them to be different.

The settings for untrusted SIP call handling (“unauthorized” or “guest” calls) must be the same across all systems in a supercluster.

The RealPresence DMA System as a SIP <-> H.323 Gateway

The RealPresence DMA system can function as a gateway for point-to-point calls between SIP and H.323 devices, whether they are registered directly to the RealPresence DMA system or to an external device. The gateway function is not used for calls to virtual meeting rooms (VMRs), virtual entry queues (VEQs), external addresses, or IP addresses.

As a best practice, Polycom recommends configuring your video conferencing network in such a way as to avoid using the RealPresence DMA system as a gateway between H.323 and SIP devices.

The gateway functionality does not support the following features:

- Media encryption
- H.239 content
- DTMF transmission

Configure SIP Settings

You can configure SIP signaling settings such as used ports, ANAT support, and device authentication.
H.323, SIP, and WebRTC signaling settings are specific to an individual cluster. When you add a cluster to a supercluster, the cluster’s signaling settings are not changed to match the settings of any other member of the supercluster. To avoid confusion, Polycom recommends that H.323, SIP, and WebRTC signaling settings be configured the same across all clusters in a supercluster, except when a specific deployment requires them to be different.

The settings for untrusted SIP call handling ("unauthorized" or "guest" calls) must be the same across all clusters in a supercluster.

To configure SIP settings

1. Go to Admin > Server > SIP Settings.
2. Select Enable SIP signaling.
3. To enable pass-through of ANAT signaling (RFC 4091 and RFC 4092) in the Session Description Protocol (SDP) for negotiating IP version in a dual-stack (IPv4 + IPv6) environment, select Enable ANAT support.
4. If the system’s security settings permit unencrypted SIP connections, optionally set Unencrypted SIP port to TCP or UDP/TCP.
   - The system only answers UDP calls if that transport is enabled. For communications back to the endpoint, it uses the transport protocol that the endpoint requested (provided that the transport is enabled, and for TCP, that unencrypted connections are permitted).
5. Enter the port numbers for the Unencrypted SIP port and TLS port. Polycom recommends keeping the default port numbers (5060 for TCP/UDP, 5061 for TLS).
6. To turn on SIP digest authentication for either the unencrypted or TLS port, select the corresponding Enable authentication check box.
   - Device authentication credentials for Inbound Authentication must be added in the Device Authentication settings.
7. Select a Dial Plan from the drop-down list for the Unencrypted SIP port and the TLS port.
8. To enable mutual TLS, select Require mutual authentication (validation of client certificates).
9. Click Update to save your settings

Configure H.323 Settings

You can configure H.323 signaling settings such as ports used, multicast, and device authentication.

H.323, SIP, and WebRTC signaling settings are specific to an individual cluster. When you add a cluster to a supercluster, the cluster’s signaling settings are not changed to match the settings of any other member of the supercluster. To avoid confusion, Polycom recommends that H.323, SIP, and WebRTC signaling settings be configured the same across all clusters in a supercluster, except when a specific deployment requires them to be different.

To configure H.323 settings

1. Go to Admin > Server > H.323 Settings.
2. Select Enable H.323 signaling.
3. Enter the port numbers for the H.225 port and RAS port. Polycom recommends keeping the default port numbers (1720 for H.225 port, 1719 for RAS port).
Signaling Settings

4. Select a **Dial Plan** from the drop-down list.
5. Select **H.323 multicast** to support gatekeeper discovery messages from endpoints.
6. Select **Enable H.323 device authentication** to turn on H.235 authentication,
   
   Device authentication credentials for **Inbound Authentication** must be added in the **Device Authentication** settings.
7. Click **Update** to save your settings.

### Configure WebRTC Settings

You can enable WebRTC signaling if you have WebRTC clients on your network.

H.323, SIP, and WebRTC signaling settings are specific to an individual cluster. When you add a cluster to a supercluster, the cluster’s signaling settings are not changed to match the settings of any other member of the supercluster. To avoid confusion, Polycom recommends that H.323, SIP, and WebRTC signaling settings be configured the same across all clusters in a supercluster, except when a specific deployment requires them to be different.

**To configure WebRTC settings**

1. Go to **Admin > Server > WebRTC Settings**.
2. Select **Enable WebRTC signaling**.
3. Select a **Dial plan** from the drop-down list.
4. Click **Update** to save your settings.

### Untrusted SIP Call Handling

You can configure special handling for SIP calls from devices outside the corporate firewall that are not registered with the RealPresence DMA system and are not from a federated division or enterprise. These calls come to the RealPresence DMA system via session border controllers (SBCs) such as a Polycom RealPresence Access Director system or Acme Packet Session Border Controller (which are configured as external SIP peers in the RealPresence DMA system).

You can route such untrusted (“unauthorized” or “guest”) calls by creating a separate set of guest dial rules used only for these untrusted calls.

You can add one or more ports so that an SBC can route untrusted calls to a specific port. For each port, you can specify whether authentication is required. You can also specify the transport, and if TLS, whether certificate validation is required (mutual TLS).

Although these are cluster-specific settings that are not part of the data store shared across superclustered systems, we strongly recommend that all signaling settings be the same across all clusters in a supercluster.

The settings for untrusted SIP call handling (“unauthorized” or “guest” calls) **must** be the same across all clusters in a supercluster.

If you add ports for untrusted calls, you must also create and associate a dial plan for those calls.
**Guest Ports**

You can maintain a list of external ports for guest users and customize the SIP settings for each, including dial plans and authentication settings.

**Add a New Guest Port**

You can add a port to the RealPresence DMA system to be used for SIP guest calls.

**To add a guest port**

1. Go to *Service Config > SIP Settings*.
2. Under *Unauthorized ports*, click the *Add* button.
3. Configure the parameters for the guest port.

4. Click *OK*.

**Edit a Guest Port**

You can edit a guest port that you have added.
To edit a guest port

1. Go to Service Config > SIP Settings.
2. Under Unauthorized ports, select the port to edit and click the Edit button.
3. Specify the port number, the transport, whether authentication is required, and for TLS, whether certificate validation is required (mutual TLS). You can also change the dial plan associated with the port.
4. Click OK.

Dial Rules for Guest Calls

If you enabled the system to receive unauthorized or guest calls, you also need to configure specific dial rules to route the unauthorized or guest calls.

The system comes with a default Guest Dial Plan to which you can add dial rules. Alternatively, you can create your own dial plan with a different name.

Add a Dial Rule for Guest Calls

You can add one or more dial rules to route unauthorized calls.

To add a dial rule for guest calls

2. Under Actions, click Add Dial Rule.
3. Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>The text description that will display under Dial Rules-Guest Dial Plan on the Dial Plans page.</td>
</tr>
<tr>
<td>Action</td>
<td>The action to be performed on unauthorized calls. When you select some actions, additional settings become available.</td>
</tr>
<tr>
<td>Enabled</td>
<td>When checked, the dial rule is active. When cleared, the rule is turned off but not deleted.</td>
</tr>
<tr>
<td>Preliminary</td>
<td>A preliminary is an executable script, written in the Javascript language, that defines processing actions (filtering or transformation) that are part of a dial rule and may be applied to a dial string before the dial rule’s action is performed. provides examples you can experiment with and modify for your purposes.</td>
</tr>
<tr>
<td>Enabled</td>
<td>When checked, the preliminary script is active. When cleared, the preliminary script is turned off but not deleted.</td>
</tr>
<tr>
<td>Script</td>
<td>Type (or paste) the preliminary script to apply to the dial string.</td>
</tr>
<tr>
<td>Debug this Script</td>
<td>Click to debug (test) the preliminary script with different variables.</td>
</tr>
</tbody>
</table>
Edit a Dial Rule for Guest Calls

Dial rules for guest calls specify how to route unauthorized calls. You can edit these dial rules as needed.

To edit a dial rule for guest calls

2. Select the guest dial rule to edit.
4. Revise the fields as described in the following table as needed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dial Rule</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>The text description that will display under Dial Rules-Guest Dial Plan on the Dial Plans page.</td>
</tr>
<tr>
<td>Action</td>
<td>The action to be performed on unauthorized calls. When you select some actions, additional settings become available.</td>
</tr>
<tr>
<td>Enabled</td>
<td>When checked, the dial rule is active. When cleared, the rule is turned off but not deleted.</td>
</tr>
<tr>
<td>Preliminary</td>
<td></td>
</tr>
<tr>
<td>Script</td>
<td>Type (or paste) the preliminary script to apply to the dial string.</td>
</tr>
<tr>
<td>Debug this Script</td>
<td>Click to debug (test) the preliminary script with different variables.</td>
</tr>
</tbody>
</table>

5. Click OK.
High Availability Settings

Two Polycom® RealPresence® DMA® systems can be configured on the same network to provide High Availability (HA) of services. Systems configured for High Availability support minimal interruption of services and greater call reliability.

In an HA configuration, each RealPresence DMA system has a virtual IP address for at least one network interface with assigned services. If one RealPresence DMA system fails, the peer system takes over the failed system’s resources (virtual IP addresses and assigned services). All active calls are either dropped automatically or callers must manually hang up, but registration and provisioning information for endpoints is maintained in memory and shared between both systems. Once all resources are re-established on the peer system, users can call back in to the video conference without changing any call information.

Although not required, Polycom recommends that you configure more than one network interface as an HA link, one of which should be a dedicated direct link. Multiple HA links provide more reliable communication between the two systems.

Network Settings to Support High Availability

When you configure the network settings for your two RealPresence DMA systems, consider the following information:

- The RealPresence DMA system supports the use of multiple network interfaces, which can be physical network interface cards (NIC), virtualized NICs (if using RealPresence DMA virtual edition) or logical network interfaces such as LACP (bonded) and VLAN (see Network Settings).
- Determine the number of interfaces your network configuration needs and identify the interfaces to use for RealPresence DMA services, dedicate exclusively to HA messaging, and/or use for both purposes.
- Assign static IP addresses to all interfaces on both nodes in the HA pair that will be used as HA links or that have services assigned. Each node must use the same interface for the same purpose (e.g., if eth0 has all services assigned to it on node A, then eth0 on node B should have all services assigned; if bond0 is an HA link on node A, it must also be an HA link on node B). Each network interface on node A must be on the same subnet as the corresponding interface on node B.
- A network interface with services assigned may also be used for HA communication
- At a minimum, configure at least one network interface for RealPresence DMA services (e.g., call signaling or administrative management) and one network interface (possibly the same one) for HA messaging between the two RealPresence DMA nodes.
- Configure the network settings for all of the network interfaces you plan to use on each system before you enable High Availability and configure its settings. Once HA is enabled, configuring network settings is disabled.
- The physical IP addresses of the same network interfaces on each system (e.g., eth1 and eth1) must be on the same subnet.
- Assign the same services to the same network interfaces on each system.
● If you plan to configure one or more network interfaces as dedicated HA links (no assigned services), you need to assign IP addresses based on the physical location of your two RealPresence DMA systems:

  ➢ If the two systems are located physically close to each other and the direct link cable does not need to be routed within your network, the IP addresses you assign to the dedicated HA interfaces do not need to be within your network IP space but they must be on the same subnet.

  ➢ If your two systems are not located in the same area, the IP addresses you assign to the dedicated HA interfaces must be within your network IP space and on the same subnet.

### High Availability Requirements

When you configure your High Availability settings, follow these requirements:

- Configure all other settings for the RealPresence DMA system identically on both systems.
- Configure one virtual IP address for each network interface that has been assigned RealPresence DMA services. If both IPV4 and IPV6 are enabled, configure one virtual IPv4 and one virtual IPV6 address.
  
  ➢ A virtual IP address must be on the same subnet as the physical IP address for the network interface.

  ➢ Use only IP addresses that are not already in use. The RealPresence DMA system does not prevent IP address conflicts and, if they occur, your HA systems will not operate correctly.

- Configure at least one network interface as an HA link. The HA link can be a LAN connection to the physical IP address of the same NIC on the peer system or it can be a direct (crossover) link. A direct link physically connects two network interfaces on a private network. Use one or both of the following settings to configure an HA link:

  ➢ **Enable Interface for HA traffic:** When enabled, the network interface can act as a dedicated HA link or it can also have assigned services. If you select this option, you must provide the physical IP address of the same NIC on the peer system.

  ➢ **Use Direct Link:** When enabled, the network interface acts as a private network HA link and cannot have assigned services.

- If a network interface is dedicated only to HA traffic (no services are assigned and it is not a direct link), assign it a virtual IP address.

- The two systems configured for High Availability use ports for UDP communication between them. HA messaging traffic must be routable if the systems do not have a direct link.

### Configure High Availability Settings

When you configure High Availability settings on one RealPresence DMA system, you can synchronize the settings to the other system by using the Configure Peer option.

Note that virtual HA settings are required only for network interfaces with assigned services. Direct links cannot have services assigned and do not require virtual IP addresses. Virtual IP addresses are tied to services but HA only communicates via physical IP addresses.

**Note:** When you configure **High Availability Interface Settings**, you need to enter the required information for each active NIC before you submit your HA settings. If you try to submit partial settings, you may have errors that result from missing information.
To configure High Availability settings:

1. Go to Admin > Server > High Availability Settings.
2. Use the information in the following table to configure the HA settings for your system.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable High Availability (HA)</td>
<td>When selected, enables HA mode.</td>
</tr>
<tr>
<td>Change HA Password</td>
<td>This option acts as an encryption key that is used to encrypt and decrypt the messages being exchanged between the two HA systems. When selected and you submit your settings, the system auto-generates a new encryption key. Note that you must then update the configuration of the peer to enable the two HA systems to communicate.</td>
</tr>
</tbody>
</table>

**High Availability Interface Settings**

<table>
<thead>
<tr>
<th>Name, IP address, and CIDR of each network interface</th>
<th>The name of each interface that is eligible for HA configuration displays along with its physical addresses (IPv4/IPv6) and their associated CIDR masks. Network interfaces that are not eligible because they are disabled also display but cannot be assigned HA settings.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configured Services</td>
<td>The RealPresence DMA system services assigned to the network interface.</td>
</tr>
<tr>
<td>HA Link</td>
<td>When enabled:</td>
</tr>
<tr>
<td></td>
<td>• The network interface serves as an HA link and communicates with the peer system via the peer’s physical IP address for the same network interface.</td>
</tr>
<tr>
<td></td>
<td>• You must enter the Peer Physical IP Address.</td>
</tr>
<tr>
<td></td>
<td>At least one network interface must be enabled as an HA link. Polycom recommends enabling at least two network interfaces as HA links, one of which should be a direct link.</td>
</tr>
<tr>
<td>Local physical IP</td>
<td>The physical IP address of the network interface being used as an HA link. If multiple local physical addresses are present (IPv4 and IPv6), select one address from the drop-down menu.</td>
</tr>
<tr>
<td>Peer physical IP</td>
<td>The peer physical address must be the same address type (IPv4/IPv6) as the local physical address. Note: This field is required on network interfaces that you enable as HA links.</td>
</tr>
<tr>
<td>Direct link</td>
<td>Select this option if you have a direct, physical link (crossover or Ethernet cable) between the same network interface on both systems. Direct Link cannot be enabled on network interfaces that have assigned services.</td>
</tr>
<tr>
<td>Gateway address</td>
<td>The gateway address for the IPv4 subnet on which the physical IP addresses are configured. This field displays only if the local and peer physical IP addresses are IPv4.</td>
</tr>
</tbody>
</table>
Configure each network interface that will be used as an HA link.

4 Click **Submit**. The system reboots.

5 After the system restarts, go to **Admin > High Availability Settings**.

6 Click **Configure Peer** to apply the same settings to the peer system.

7 Complete the following fields (all are required):

   - **Peer IP**: Enter the management IP address of the peer RealPresence DMA system.
   - **Peer Port**: Port 8443 is the default port for the peer system.
   - **Peer Admin Account**: The username that the peer system administrator uses to log in to the system’s web user interface.
   - **Peer Admin Password**: The peer system administrator’s login password.
   - Click **OK**.

### Change High Availability Password

When you configure two RealPresence DMA systems for High Availability, the two systems share an internal account that supports authentication between the systems. The account does not require any interaction. However, if your network policy requires you to change passwords at certain intervals, you can use the **Change HA Password** option.

**Caution**: Change the HA password only when both systems have no active calls. Otherwise, all active calls will be dropped when you submit the changes from the High Availability Settings page.
To change the high availability password:

1. Go to Admin > Server > High Availability Settings.
2. Select Change HA Password.
3. Click Submit.
   The system reboots.
4. After the system restarts, go to Admin > Server > High Availability Settings.
5. Click Configure Peer.
6. Enter the name and password and click OK.
   The peer system reconnects and all HA settings are applied to the peer system, including the new password.

High Availability Licensing

Polycom recommends that you license each server or allocate each virtual instance with the same number of calls. The RealPresence DMA systems within an HA pair will pool the number of licensed calls, so each individual system can be licensed for half of the total number of calls you must be able to support at any given time. If the active system in an HA pair fails, the standby system can support the total number of calls licensed for both systems for a period of two weeks. If the formerly active system that failed is not repaired or replaced within that time, the standby system will lose access to the call licenses that were allocated to the formerly active system.

For instructions on activating your licenses, see Licensing in the Polycom® RealPresence® DMA® System Operations Guide.

Certificates for High Availability Systems

When you deploy two RealPresence DMA systems for High Availability, each system has a default self-signed SSL certificate. To ensure that both of your systems are identified as trusted entities, Polycom recommends that you request signed identity certificates from a Certificate Authority (CA). Each RealPresence DMA system should have a certificate that includes the virtual IP address and virtual hostname and the physical IP address and hostname.

After you receive the signed certificates, you need to install them on both RealPresence DMA systems after you enable and configure network and High Availability settings. Additionally, you need to install your chosen CA's public certificate on each system.

Note that if you upgrade your HA nodes to a new version of the RealPresence DMA software, each system automatically generates and installs a new self-signed certificate. The new certificate replaces any self-signed or signed certificates that you previously installed. After upgrading, you need to submit a new Certificate Signing Request (CSR) for each system to obtain signed certificates.

Note: When you make changes in the RealPresence DMA system that cause a new certificate to be generated, or when you install a new certificate, you may need to refresh or reload your browser before you log back in to the management user interface.

If you refresh your browser and still see outdated information or cannot download log files in the RealPresence DMA system, you need to clear your browser’s cache.
See Security Certificates for more information about certificates.

**Requesting Signed Certificates**

After you configure the network and High Availability settings, you need to submit Certificate Signing Requests (CSRs) to obtain a signed certificate for each system. Each CSR must include the FQDN and domain of the individual RealPresence DMA system and Subject Alternative Names (SANs) for the following:

- Virtual hostnames for interfaces on the individual RealPresence DMA system
- Virtual IP addresses for interfaces on the individual RealPresence DMA system
- Virtual hostnames for interfaces on the peer RealPresence DMA system
- Virtual IP addresses for interfaces on the peer RealPresence DMA system

After you receive the signed certificates, install both certificates in the KEY_STORE of both RealPresence DMA systems.

**Integrating High Availability Systems with the RealPresence Resource Manager System**

If you plan to integrate your RealPresence DMA High Availability systems with a RealPresence Resource Manager system, configure the network settings on both HA nodes and enable and configure the HA settings before you integrate with the RealPresence Resource Manager system. After the systems are integrated, you need to create three entries in the RealPresence Resource Manager system for the RealPresence DMA system HA pair as follows:

- One entry must point the RealPresence Resource Manager system to the virtual IP address of the HA pair to integrate network and site topology information.
- Two entries must point the RealPresence Resource Manager system to the physical IP address of each system in the HA pair to obtain license information.

**DNS Records for High Availability**

Your RealPresence DMA systems must be accessible by their host name(s), not just their IP address(es), so you (or your DNS administrator) must create the necessary A (and/or AAAA) records, as well as the corresponding PTR records, on your DNS server(s).

A (IPv4) and AAAA (IPv6) records map each physical host name to the corresponding physical IP address and each virtual host name to the corresponding virtual IP address. The corresponding PTR records allow reverse DNS resolution of the system's physical or virtual host name(s).

For further details about DNS records required for the RealPresence DMA system, see in .

**Note:** Depending on local DNS configuration, a host name could be the RealPresence DMA system's fully qualified domain name (FQDN) or a shorter name that DNS can resolve.
Licenses

A Polycom RealPresence DMA system's license specifies the maximum number of concurrent calls that can touch the system.

In a supercluster configuration, note the following:

- A single call may touch more than one system. The call consumes a license on each system it touches.
- Each system may be licensed for a different number of calls.
- If your superclustering strategy calls for a system to be primary for one territory and backup for another, it must be licensed for the call volume expected if it has to take over the territory for the primary system.
- License pooling is available across a supercluster or High Availability pair. Any system can share all licenses on all servers in all clusters.

The licensing process depends on the type of license you have for your product. Within the management user interface, you can enable licensing with activation keys or you can specify a licensing server.

- If you are a Polycom RealPresence Clariti™ customer with a Polycom RealPresence Resource Manager system version 10.0 or later, you must use the RealPresence Resource Manager system to license your product. If you have not deployed a RealPresence Resource Manager system or if you have not upgraded your RealPresence Resource Manager system to version 10.0 or later, you must license your product using the RealPresence Platform Director system version 3.0 or later.
- If you are not a RealPresence Clariti customer, you must use a license file to obtain an activation key code to license your product.

You can also switch from using a license with an activation key to using a license server. Note that if you do so, you cannot switch back to using a license that requires an activation key.

View License Information

The licensing information that you can view for your system varies slightly based on whether you have a RealPresence DMA Appliance Edition or Virtual Edition.

To view license information:

1. Go to Admin > Server > Licenses.
2. View the fields on the Licenses page as described in the following table:
Adding Licenses

You can add licenses to both Appliance Edition and Virtual Edition systems.

**Adding a License to the RealPresence DMA System, Appliance Edition**

If you have a RealPresence DMA system, Appliance Edition, and are not a Polycom RealPresence Clariti™ customer, you need to complete the following two-step process to license your system:

- Request a software activation key code for the server.
- Enter the activation key code into the system’s management user interface.
Request a Software Activation Key Code for the Server

To license an Appliance Edition system, you need to request an activation key code for the server you need to license.

**Caution:** An activation key is linked to a specific server’s serial number. For a two-server cluster, you must generate the activation key for each server using that server’s serial number. Licensing will fail if you generate both activation keys from the same server serial number.

**To request a software activation key code for each server**

1. Log into the RealPresence DMA system as an administrator and go to Admin > Server > Licenses.
2. Record the serial number for the RealPresence DMA server.
4. If you don’t already have one, register for an account and log in.
5. Select Licensing & Product Registration > Activation/Upgrade.
   A product selection window displays.
6. Select All other Polycom Products.
7. Select SITE & Single Activation / Upgrade.
8. In the Serial Number field, enter the server’s serial number.
9. In the License Number field, enter the software license number listed on the server’s License Certificate (shipped with the product).
10. Click Generate.
11. Record the activation key for the server.
12. If you have a two-server cluster, repeat steps 8-11, this time entering the second license number you received and the second server’s serial number.

**Enter a License Activation Key Code**

Complete system licensing by entering the new activation key code on the Licenses page.

**To enter a license activation key code**

1. Go to Admin > Server > Licenses.
2. In the Primary key field, enter the activation key code that was generated for the server’s serial number.
3. Click Update.
   The license is updated.
4. Click OK.

---

**Caution:** An activation key is linked to a specific server’s serial number. For a two-server cluster, you must generate the activation key for each server using that server’s serial number. Licensing will fail if you generate both activation keys from the same server serial number.
Adding a License to the RealPresence DMA System Using the RealPresence Resource Manager System

If you are a Polycom RealPresence Clariti™ customer, you need to license your RealPresence DMA Appliance Edition or Virtual Edition through the Polycom RealPresence Resource Manager system, version 10.0 or higher. If you do not have a RealPresence Resource Manager system, you must license your RealPresence DMA system through the Polycom RealPresence Platform Director system.

See the Polycom RealPresence Resource Manager Operations Guide for licensing instructions (available at support.polycom.com).
Security Settings

The Polycom® RealPresence® DMA® system security settings enable you to switch between enhanced security mode and a custom security mode in which you can enable one or more insecure network access capabilities. Polycom recommends that you use the enhanced security mode unless you have a specific need to allow one of the insecure capabilities.

Selecting a Security Mode

When you select **Enhanced security** mode, all **Custom security** mode options are unchecked and disabled. You can still configure some settings that can be applied to either security mode.

When you select **Custom security** mode, all custom options are unchecked by default. You can then select the specific capabilities you need for network access to your RealPresence DMA system environment.

Whether you use enhanced or custom security mode, your settings are not locked and the ability to lock settings is not supported. You can switch to the other security mode when necessary for your environment.

**Note:** All systems in a supercluster must have the same security settings. If you invite a system to join an existing supercluster, the invited system’s security settings will be changed to match those of the supercluster. You cannot change a system’s security settings while it is part of a supercluster.

Configure Security Settings

When you configure security settings, you can select the system’s security level and configure various network access settings.

**Caution:** If you select SSL 3.0 as a security protocol for HTTPS communication, but do not select at least one TLS protocol (TLS 1.0, TLS 1.1, or TLS 1.2), you may not be able to access the RealPresence DMA web user interface in most browsers. Polycom recommends selecting at least one TLS protocol.

**To configure security settings:**

1. Go to **Admin > Server > Security Settings**.
2. Select the security settings needed for your system as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enhanced security</strong></td>
<td>When selected, this mode disables all <strong>Custom security options</strong> (unencrypted protocols and non-essential system access methods).</td>
</tr>
<tr>
<td><strong>Custom security</strong></td>
<td>When selected, this mode enables you to select one or more of the unsecured methods of network access listed in the check boxes.</td>
</tr>
<tr>
<td><strong>Allow Linux console access</strong></td>
<td>Enables the Linux user root to log into the system using SSH. This direct Linux access is not needed for normal operation, routine maintenance, or even troubleshooting, all of which can be done through the administrative user interface. In certain situations, this option might enable Polycom Global Services personnel to more fully understand the state of a troubled system or correct problems. Enable this option only when asked to do so by Polycom Global Services.</td>
</tr>
<tr>
<td><strong>Allow unencrypted connections to the Active Directory</strong></td>
<td>The Polycom RealPresence DMA system connects to Active Directory using SSL or TLS encryption. However, if the Active Directory server or servers (including domain controllers if you import global groups) are not configured to support encryption, the RealPresence DMA system can only connect using an unencrypted protocol. This option allows such connections if an encrypted connection cannot be established. When selected, the unencrypted passwords of enterprise users are transmitted over the network. Use this option only for diagnostic purposes. By toggling it, you can determine whether encryption is the cause of a failure to connect to Active Directory or to load group data. If so, the solution is to correctly configure the relevant servers, not to allow ongoing use of unencrypted connections.</td>
</tr>
<tr>
<td><strong>Allow unencrypted connections to MCUs</strong></td>
<td>The Polycom RealPresence DMA system uses only HTTPS for the conference control connection to RealPresence Collaboration Server or RMX MCUs, and therefore cannot control an MCU that accepts only HTTP (the default). This option enables the system to fall back to HTTP for MCUs not configured for HTTPS. Polycom recommends configuring your MCUs to accept encrypted connections rather than enabling this option. When unencrypted connections are used, the RealPresence Collaboration Server or RMX login name and password are sent unencrypted over the network.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Allow basic authentication to Exchange server | If calendaring is enabled, the Polycom RealPresence DMA system authenticates itself with the Exchange server using NTLM authentication.
If this option is selected, the Polycom RealPresence DMA system still attempts to use NTLM first, but if it fails or is not enabled on the Exchange server, then the RealPresence DMA system falls back to HTTP Basic authentication (user name and password).
Polycom recommends using NTLM authentication rather than enabling this option.
For either NTLM or HTTP Basic authentication to work, they must be enabled on the Exchange server.

Unlock SIP Settings mutual authentication option on the SIP Settings page | During encrypted call signaling (SIP over TLS), the Polycom RealPresence DMA system requires the remote party (endpoint or MCU) to present a valid certificate. This is known as mutual TLS.
When selected, this option unlocks the **Require mutual authentication (validation of client certificates)** check box for SIP signaling when you Configure SIP Settings, allowing you to disable the mutual TLS requirement for SIP signaling.
Polycom recommends installing valid certificates on your endpoints and MCUs rather than enabling this option.

Allow third-party applications to receive SIP RFC 4575 conference events | The SIP SUBSCRIBE/NOTIFY conference notification service (as described in RFCs 3265 and 4575), allows SIP devices to subscribe to a conference and receive conference rosters and notifications of conference events. Normally, the subscribing endpoints are conference participants.
This option configures the system to let devices subscribe to a conference without being participants in the conference.
**Note:** A subscription to a conference by a non-participant consumes a call license. Call history does not include data for non-participant subscriptions.

Use non-FIPS mode (change will cause system restart) | When selected, non-FIPS-compliant protocols and access methods are supported.
Federal Information Processing Standards (FIPS) are standards developed by the United States federal government for use in computer systems by non-military government agencies and government contractors. The standards establish requirements for various purposes, such as ensuring computer security and interoperability, and are intended for cases in which suitable industry standards do not already exist.
When the check box is cleared, the system uses FIPS mode and the **Skip validation of certificates received while making outbound connections** check box is automatically cleared and disabled. When in FIPS mode, validation of certificates is mandatory.
### Security Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Skip validation of certificates received while making outbound connections | When the RealPresence DMA system connects to a server, it validates that server’s certificate. This option configures the system to accept any certificate presented to it without validating it. Polycom recommends using valid certificates for all servers that the system may need to contact rather than enabling this option. Depending on system configuration, this may include:  
  - MCUs  
  - Active Directory  
  - Exchange  
  - RealPresence Resource Manager system  
  - Other RealPresence DMA systems  
  - Endpoints  
  
  **Note:** Either the Common Name (CN) or Subject Alternative Name (SAN) field of the server’s certificate must contain the address or host name that the RealPresence DMA system specifies for that server. For example, if the RealPresence DMA system is integrated with an Active Directory system with the FQDN `DC.myenterprise.com`, then the RealPresence DMA system will validate that the certificate it receives has either a CN or SAN entry for `DC.myenterprise.com`. Polycom MCUs do not include their management IP address in the SAN field of the Certificate Signing Request (CSR), so their certificates identify them only by the CN. Therefore, in the RealPresence DMA system, an MCU's management interface must be identified by the name specified in the CN field (usually the FQDN), not by IP address. Similarly, an Active Directory server certificate often specifies only the FQDN. So in the RealPresence DMA system, identify the enterprise directory by FQDN, not by IP address. |
| Allow system booting from USB or optical drive (does not apply to RealPresence DMA Virtual Edition) (change will cause system restart) | When selected, the system can be booted from a USB device or an optical drive. If this check box is cleared, the boot order is configured so that the server cannot be booted from a USB device or the optical drive. |

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Skip validation of certificates for inbound connections | This option affects inbound connections from entities like web browsers and API clients. If this check box is cleared, you can only connect to the RealPresence DMA system if your browser presents a client certificate issued by a CA that the system trusts (this is known as mutual TLS for administrative connections). Clear this check box only if:  
  - You have implemented a complete public key infrastructure (PKI) system, including a CA server, client software (and optionally hardware, tokens, or smartcards), and the appropriate operational procedures.  
  - The CA's public certificate is installed in the RealPresence DMA system so that it trusts the CA.  
  - All authorized users, including yourself, have a client certificate signed by the CA that authenticates them to the RealPresence DMA system. |

---

The following settings may be configured in any security mode

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Skip validation of certificates for inbound connections | This option affects inbound connections from entities like web browsers and API clients. If this check box is cleared, you can only connect to the RealPresence DMA system if your browser presents a client certificate issued by a CA that the system trusts (this is known as mutual TLS for administrative connections). Clear this check box only if:  
  - You have implemented a complete public key infrastructure (PKI) system, including a CA server, client software (and optionally hardware, tokens, or smartcards), and the appropriate operational procedures.  
  - The CA's public certificate is installed in the RealPresence DMA system so that it trusts the CA.  
  - All authorized users, including yourself, have a client certificate signed by the CA that authenticates them to the RealPresence DMA system. |
3 Click **Update** to save the settings.

### Restrict Security Ciphers

The RealPresence DMA system comes with default ciphers enabled for each security protocol that you allow. The ciphers for each security protocol are applied to communication that occurs on the management network interface and/or the signaling network interface.

You can restrict the ciphers for the security protocols that you allow, but Polycom recommends that you use the default settings unless you are knowledgeable about ciphers and the consequences of removing specific ciphers.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow forwarding of IPv6 ICMP destination unreachable messages</td>
<td>When this check box is cleared, the RealPresence DMA system has an internal firewall rule that blocks outbound destination unreachable messages. When selected, the internal firewall rule is disabled. <strong>Note:</strong> The RealPresence DMA system currently does not send such messages, regardless of this setting.</td>
</tr>
<tr>
<td>Allow IPv6 ICMP echo reply messages to multicast addresses</td>
<td>When this check box is cleared, the RealPresence DMA system does not reply to echo request messages sent to multicast addresses (multicast pings). When selected, the system responds to multicast pings.</td>
</tr>
<tr>
<td>Ignore SIP “critical” privacy flag</td>
<td>When selected, the RealPresence DMA system ignores the “critical” flag in the Privacy header of incoming SIP messages, and accepts calls marked with this flag. When this check box is cleared, the system rejects incoming calls that include a “critical” flag in the Privacy header and sends a 500 response code.</td>
</tr>
<tr>
<td>Remove “critical” flag</td>
<td>If you select the <strong>Ignore SIP “critical” privacy flag</strong> check box, this option (when selected) instructs the RealPresence DMA system to remove the “critical” flag from the Privacy header of incoming SIP messages. If the Privacy header has no remaining flags after the “critical” flag is removed, the system removes the Privacy header from the message.</td>
</tr>
<tr>
<td>Allow SSL 3.0</td>
<td>When selected, allows the system to support the SSL 3.0 protocol for HTTPS communication. Disabled by default. Changing this setting causes the system to restart.</td>
</tr>
<tr>
<td>Allow TLS 1.0</td>
<td>When selected, allows the system to support the TLS 1.0 protocol for HTTPS communication. Enabled by default. Changing this setting causes the system to restart.</td>
</tr>
<tr>
<td>Allow TLS 1.1</td>
<td>When selected, allows the system to support the TLS 1.1 protocol for HTTPS communication. Enabled by default. Changing this setting causes the system to restart.</td>
</tr>
<tr>
<td>Allow TLS 1.2</td>
<td>When selected, allows the system to support the TLS 1.2 protocol for HTTPS communication. Enabled by default. Changing this setting causes the system to restart.</td>
</tr>
</tbody>
</table>
To restrict security ciphers:

1. Go to Admin > Server > Security Settings.
2. Click Management Cipher Selection to choose the ciphers to be applied on the management interface based on the allowed security protocols, as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the cipher.</td>
</tr>
<tr>
<td>Class</td>
<td>The classes of security that include the cipher.</td>
</tr>
<tr>
<td>Security protocol and FIPS mode</td>
<td></td>
</tr>
<tr>
<td>TLS 1.0</td>
<td>Lists the security protocols and FIPS mode. Yes and No indicate whether the protocol or FIPS mode uses the individual ciphers.</td>
</tr>
<tr>
<td>TLS 1.1</td>
<td></td>
</tr>
<tr>
<td>TLS 1.2</td>
<td></td>
</tr>
<tr>
<td>SSL V3</td>
<td></td>
</tr>
<tr>
<td>FIPS</td>
<td></td>
</tr>
<tr>
<td>Default</td>
<td>Indicates whether the cipher is enabled as a RealPresence DMA system default setting for the different security protocols and FIPS mode. If you modify the ciphers that are selected, you can use the Yes and No indicators in this column to reconfigure your settings to the original defaults if necessary.</td>
</tr>
</tbody>
</table>

3. Click Signaling Cipher Selection to choose the ciphers to be applied on the signaling interface based on the allowed security protocols, as described in the preceding table.
4. Click Update to save the settings.
Security Certificates

Certificates are used between systems within your video conferencing environment (such as servers and endpoints) to build a trust/authentication and to support encryption. Certificates confirm that the servers within your infrastructure can communicate and have the option to encrypt the data. Each digital certificate is identified by its public key. The collection of all public keys used in an enterprise to determine trust is known as a Public Key Infrastructure (PKI).

The certificate authority, or CA, or is a single, centralized authority such as an enterprise’s IT department or a commercial certificate authority that each computer on the network is configured to trust. Each server on the network has a public certificate that identifies it. When a client connects to a server, the server shows its signed public certificate to the client. The certificate authority signs the public certificates of those servers that clients should trust. Trust is established because the certificate has been signed by the certificate authority, and the client has been configured to trust the CA.

How Certificates Are Used

The Polycom® RealPresence® DMA® system uses certificates in the following ways:

1. The Polycom® RealPresence® DMA® system presents its certificate to the remote end. For example:
   - When a user logs into the RealPresence DMA system’s browser-based management interface, the RealPresence DMA system offers a certificate to identify itself to the browser (client).
     The RealPresence DMA system’s certificate must have been signed by a certificate authority and the browser must be configured to trust that certificate authority.
     If trust cannot be established, most browsers allow connection anyway, but display a dialog to the user, requesting permission.
   - When the RealPresence DMA system connects to a Microsoft Active Directory server, it may present a certificate to the server to identify itself.
     If Active Directory is configured to require a client certificate (this is not the default), the RealPresence DMA system offers the same SSL server certificate that it offers to browsers connecting to the system management interface. Active Directory must be configured to trust the certificate authority, or it rejects the certificate and the connection fails.
   - When the RealPresence DMA system connects to a Microsoft Exchange server (if the calendaring service is enabled), it may present a certificate to the server to identify itself.
     Unless the Allow unencrypted calendar notifications from Exchange server security option is enabled, the RealPresence DMA system offers the same SSL server certificate that it offers to browsers connecting to the system management interface. The Microsoft Exchange server must be configured to trust the certificate authority. Otherwise, the Microsoft Exchange Server integration status remains Subscription pending indefinitely, the Polycom RealPresence DMA system does not receive calendar notifications, and incoming meeting request messages are only processed approximately every 4 minutes.
The RealPresence DMA system validates the certificate of a remote server. For example:

- When the RealPresence DMA system connects to a Polycom MCU configured for secure communications, a certificate may be used to identify the MCU (server) to the RealPresence DMA system (client). This can be configured in the RealPresence DMA system.

- When performing call signaling requiring TLS, the RealPresence DMA system presents its certificate to the connecting client (one-way TLS). If the **Require mutual authentication (validation of client certificates)** SIP Settings option is enabled, the both ends validate each other’s certificates (mutual TLS).

The RealPresence DMA system validates the certificate of a client. For example:

For incoming SIP connections, the RealPresence DMA system may check the client’s certificate. This can be configured in the RealPresence DMA system (see [Selecting a Security Mode](#)).

## Accepted Certificates

Certificates come in several forms (encoding and protocol). The following table shows the forms that can be installed in the RealPresence DMA system.

<table>
<thead>
<tr>
<th>Encoding</th>
<th>Protocol / File Type</th>
<th>Description and Installation Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>PEM (Base64-encoded ASCII text)</td>
<td>PKCS #7 protocol P7B file</td>
<td>Certificate chain containing: • A signed certificate for the system, authenticating its public key. • The CA's public certificate. • Sometimes intermediate certificates. Upload file or paste into text box.</td>
</tr>
<tr>
<td>CER (single certificate) file</td>
<td>Signed certificate for the system, authenticating its public key. Upload file or paste into text box.</td>
<td></td>
</tr>
<tr>
<td>Certificate text</td>
<td>Encoded certificate text copied from CA's email or secure web page. Paste into text box.</td>
<td></td>
</tr>
</tbody>
</table>
Certificate Signing Requests

The initial RealPresence DMA system configuration permits using the default, self-signed certificate. Normal operation in a secure mode requires that you install a digital certificate signed by a trusted certificate authority that uniquely identifies the RealPresence DMA system within your public key infrastructure. This can be done by creating a certificate signing request for the RealPresence DMA system and submitting it to a certificate authority to be signed.

Although it is common for a system to be identified by any number of digital certificates, each signed by a different CA, the RealPresence DMA system currently supports only a single identity certificate.

Note: Although it is common for a system to be identified by any number of digital certificates, each signed by a different CA, the RealPresence DMA system currently only supports a single identity certificate.

This section includes the following topics:
- Certificate Signing Request Requirements
- Create a Certificate Signing Request

Certificate Signing Request Requirements

When you create a certificate signing request (CSR) from the Admin > Server > Certificates page, the system populates the CSR with the data that you enter in the Certificate Information dialog, including Subject Alternative Name (SAN) extensions. The default system-generated SAN extensions, which may vary depending on your configuration, are shown in the Value list. You can change these values or add more
extensions if needed. Polycom recommends that you do not delete the default SAN extensions as the resulting certificate may not work with your configuration.

**Note: FQDN recommended for domain names**
Polycom recommends the use of the system’s fully qualified domain name (FQDN) for required SAN-DNS extensions. Newer CA regulations may cause your CA to reject the CSR if only short host names are used.

When you create a CSR, if you include the SAN extensions listed in the *Optional Fields* column, the resulting certificate will allow users to access the system using an abbreviated name without authentication errors. Ensure that you use a CA that can accept all of the CSR fields and SAN extensions required for your configuration. The following table lists required and optional fields for single-server, clustered, and superclustered configurations.

**Required and Optional CSR Fields**

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Required Fields</th>
<th>Optional Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single-server system</td>
<td></td>
<td>SA-N: Host name</td>
</tr>
<tr>
<td>• Common Name: Fully qualified domain name (FQDN)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• SAN-DNS: FQDN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• SAN-DNS: System IP address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• SAN-IP: System IP address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Country</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Two-server cluster</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Single-server system in a supercluster</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Two-server cluster in a supercluster</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Common Name: Virtual fully qualified domain name (FQDN)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• SAN-DNS: Virtual FQDN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• SAN-DNS: Physical server 1 FQDN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• SAN-DNS: Physical server 2 FQDN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• SAN-DNS: Virtual IP address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• SAN-DNS: Physical server 1 IP address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• SAN-DNS: Physical server 2 IP address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• SAN-IP: Virtual IP address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• SAN-IP: Physical Server 1 IP address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• SAN-IP: Physical Server 2 IP address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Country</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Create a Certificate Signing Request**

The following procedure creates a certificate signing request (CSR) that you can submit to your chosen certificate authority. This method uses the private key generated at software installation time.
Note: Obtaining certificates for Microsoft environments
If you’re configuring the Polycom RealPresence DMA system to support Polycom’s solution for the Microsoft OCS or Skype for Business environment, you can use Microsoft’s Certificate Wizard to request and obtain a PFX file (a password-protected PKCS12 file containing a private key and public key for the system, and the CA's certificate). See Polycom’s Microsoft Solution Deployment Guide, available at support.polycom.com, for information about using the Certificate Wizard.

To create a certificate signing request

1 Go to Admin > Server > Certificates.
   By default, the system is configured to use a self-signed certificate.

2 To see details of the public certificate currently being used to identify the system to other computers:
   a In the list, select the Server SSL certificate.
   b In the Actions list, select Display Details.
      The Certificate Details dialog appears. If this is the default self-signed certificate, Organizational Unit is Self Signed Certificate.
   c To close the dialog, click OK.

3 In the Actions list, select Create Certificate Signing Request.
   If you’ve created a signing request before, you’re asked if you want to use your existing certificate request or generate a new one. Elect to generate a new one.

4 Enter the identifying information for your Polycom RealPresence DMA system as described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common name (CN)</td>
<td>Defaults to the FQDN of the system’s management interface, as defined by the virtual host name and domain specified on the Network page. Editable.</td>
</tr>
<tr>
<td>Signature algorithm</td>
<td>The cryptographic hash algorithm used to sign the CSR.</td>
</tr>
<tr>
<td>Organizational unit (OU)</td>
<td>Subdivision of organization. Specify up to three OUs. Optional.</td>
</tr>
<tr>
<td>Organization (O)</td>
<td>Optional.</td>
</tr>
<tr>
<td>City or locality (L)</td>
<td>Optional.</td>
</tr>
<tr>
<td>State (ST)</td>
<td>Optional.</td>
</tr>
<tr>
<td>Country (C)</td>
<td>Two-character country code.</td>
</tr>
<tr>
<td>Subject Alternative Name (SAN)</td>
<td>The area you can use to add, edit, or delete SAN extensions in this CSR.</td>
</tr>
<tr>
<td>Value</td>
<td>A list of SAN extensions and their values currently associated with the CSR.</td>
</tr>
</tbody>
</table>

5 Click Add to open the Add Subject Alternative Name (SAN) dialog.
6 Select an Extension type from the list and enter the associated Extension value.
7 Click OK to close the dialog.
8. Repeat steps 5-7 as needed to add SAN extensions required for your configuration.

9. To change an existing SAN extension, select it from the Value list and click Edit.

10. To delete a SAN value, select it from the Value list and click Delete.

11. Click OK to generate the CSR.

   The Certificate Signing Request dialog displays the encoded request.

12. Copy the entire contents of the Encoded Request box (including the text "-----BEGIN NEW CERTIFICATE REQUEST----- and -----END NEW CERTIFICATE REQUEST-----") and submit it to your certificate authority.

   Depending on the certificate authority, your CSR may be submitted via email or by pasting into a web page.

13. Click OK to close the dialog.

   When your certificate authority has processed your request, it sends you a signed public certificate for your RealPresence DMA system. Some certificate authorities also send intermediate certificates and/or root certificates. Depending on the certificate authority, these certificates may arrive as e-mail text, e-mail attachments, or be available on a secure web page.

   The Polycom RealPresence DMA system accepts PKCS#7 or PKCS#12 certificate chains or single certificates.

   Caution: Some CSR fields should not be modified
   When you submit the CSR to your CA, make sure that the CA doesn't modify any of the predefined SAN fields or the X.509v3 Key Usage or Extended Key Usage fields. Changes to these fields may make your system unusable.

**View an Encoded Certificate Signing Request**

You can view an encoded certificate signing request and copy it for submittal to your certificate authority.

**To view an encoded certificate signing request**

1. Ensure the information in the Summary section is correct.

2. In the Encoded Request box, select and copy the encoded certificate request text, if desired.

3. Click OK.

**Add a Subject Alternative Name (SAN) Extension**

You can add a SAN extension when you create a certificate signing request.

**To add a SAN extension**

1. Go to Admin > Server > Certificates.

2. Click Create Certificate Signing Request.

3. Enter any required certificate information in the appropriate fields.

4. In the Subject Alternative Name (SAN) area, click Add.

5. Enter information in the following fields as required.
Edit a Subject Alternative Name (SAN) Extension

You can edit an existing SAN extension when you create a certificate signing request.

To edit a SAN extension

1. Go to Admin > Server > Certificates.
2. Click Create Certificate Signing Request.
3. Enter any required certificate information in the appropriate fields.
4. In the Subject Alternative Name (SAN) area, click Edit.
5. Change information in the following fields as required.

### Installing Certificates

You can add, edit, and remove certificates from the system.

**Note:** When you make changes in the RealPresence DMA system that cause a new certificate to be generated, or when you install a new certificate, you may need to refresh or reload your browser before you log back in to the management user interface. If you refresh your browser and still see outdated information or cannot download log files in the RealPresence DMA system, you need to clear your browser’s cache.

This section includes the following topics:

- View Installed Certificates
- Display Certificate Details
- Install a Certificate Authority's Certificate
- Install a Signed Certificate
View Installed Certificates

You can view installed certificates on the Certificates Settings page.

To view installed certificates

» Go to Admin > Server > Certificates.

The list of installed certificates appears, as described by the following table.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable OCSP</td>
<td>Enables the use of Online Certificate Status Protocol as a means of obtaining the revocation status of a certificate presented to the system. If <strong>OCSP responder URL</strong> is not specified, the system checks the certificate’s AuthorityInfoAccess (AIA) extension fields for the location of an OCSP responder: • If there is none, the certificate fails validation. • Otherwise, the system sends the OCSP request to the responder identified in the certificate. If <strong>OCSP responder URL</strong> is specified, the system sends the OCSP request to that responder. The responder returns a message indicating whether the certificate is good, revoked, or unknown. If <strong>OCSP certificate</strong> is specified, the response message must be signed by the specified certificate’s private key.</td>
</tr>
<tr>
<td>OCSP responder URL</td>
<td>Identifies the responder to be used for all OCSP requests, overriding the AIA field values. If <strong>OCSP certificate</strong> is specified, the response message must be signed by the specified certificate’s private key.</td>
</tr>
<tr>
<td>OCSP certificate</td>
<td>Select a certificate to require OCSP response messages to be signed by the specified certificate’s private key.</td>
</tr>
<tr>
<td>Store OCSP Configuration</td>
<td>Saves the OCSP configuration.</td>
</tr>
<tr>
<td>Identifier</td>
<td>Common name of the certificate.</td>
</tr>
<tr>
<td>Purpose</td>
<td>Kind of certificate: • Server SSL is the RealPresence DMA system’s public certificate, which it presents to identify itself. By default, this is a self-signed certificate, not trusted by other devices. • Trusted Root CA is the root certificate of a certificate authority that the RealPresence DMA system trusts. • Intermediate CA is a CA certificate that trusted root CAs issue themselves to sign certificate signing requests (reducing the likelihood of their root certificate being compromised). If the RealPresence DMA system trusts the root CA, then the chain consisting of it, its intermediate CA certificates, and the server certificate will all be trusted.</td>
</tr>
<tr>
<td>Expiration</td>
<td>Expiration date of certificate.</td>
</tr>
</tbody>
</table>
Display Certificate Details

You can select a certificate from the list of installed certificates and view its information.

To display certificate details

1. Go to Admin > Server > Certificates.
2. Select a certificate from the list and click Display Details.
3. View the certificate details, as outlined in the following table.

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Info</td>
<td>Purpose and alias of the certificate.</td>
</tr>
<tr>
<td>Issued To</td>
<td>Information about the entity to which the certificate was issued and the certificate serial number.</td>
</tr>
<tr>
<td>Issued By</td>
<td>Information about the issuer.</td>
</tr>
<tr>
<td>Validity</td>
<td>Issue and expiration dates.</td>
</tr>
<tr>
<td>Fingerprints</td>
<td>SHA1 and MD5 fingerprints (checksums) for confirming certificate.</td>
</tr>
<tr>
<td>Subject Alternative Names</td>
<td>Additional identities bound to the subject of the certificate. For the Polycom RealPresence DMA system, this should include the virtual and physical FQDNs, short host names, and IP addresses of the system.</td>
</tr>
<tr>
<td>Extended Key Usage</td>
<td>Indicates the purposes for which the certificate can be used. The Polycom RealPresence DMA system’s certificate is used for both server and client connections, so this should always contain at least serverAuth and clientAuth.</td>
</tr>
</tbody>
</table>

4. When finished viewing the certificate details, click OK.

Install a Certificate Authority’s Certificate

This procedure is not necessary if you obtain a certificate chain that includes a signed certificate for the Polycom RealPresence DMA system, your certificate authority’s public certificate, and any intermediate certificates.

Use this procedure to add a trusted certificate authority, either an in-house or commercial CA.

Caution: Installing or removing certificates requires a restart

Installing or removing certificates requires a system restart and terminates all active conferences. When you install or remove a certificate, the change is made to the certificate store immediately, but the system can’t implement the change until it restarts and reads the changed certificate store. For your convenience, you’re not required to restart and apply a change immediately. This permits you to perform multiple installs or removals before restarting and applying the changes. But when you’re finished making changes, you must select Restart to Apply Saved Changes to restart the system and finish your update. Before you begin, make sure there are no active conferences and you’re prepared to restart the system when you’re finished.
To install a certificate for a trusted root CA

1. Go to Admin > Server > Certificates.

   The installed certificates are listed. The Trusted Root CA entries, if any, represent the certificate authorities whose public certificates are already installed on the RealPresence DMA system and are thus trusted.

2. If you’re using a certificate authority that isn’t listed, obtain a copy of your certificate authority’s public certificate.

   The certificate must be either a single X.509 certificate or a PKCS#7 certificate chain. If it’s ASCII text, it’s in PEM format, and starts with the text -----BEGIN CERTIFICATE-----. If it’s a file, it can be either PEM or DER encoded.

3. In the Actions list, select Add Certificates.

4. In the Add Certificates dialog, do one of the following:
   
   - If you have a file, click Upload certificate, enter the password (if any) for the file, and browse to the file or enter the path and file name.
   
   - If you have PEM-format text, copy the certificate text, click Paste certificate, and paste it into the text box below.

5. Click OK.

6. Verify that the certificate appears in the list as a Trusted Root CA.

7. Click Restart to Apply Saved Changes, and when asked to confirm that you want to restart the system so that certificate changes can take effect, click OK.

Install a Signed Certificate

Before installing a certificate or certificate chain provided by the certificate authority, be sure that you received the certificate or certificate chain in one of the following forms:

- A PFX, P7B, or single certificate file that you have saved on your computer.
- PEM-format encoded text that you received in an e-mail or on a secure web page.

Installing or removing certificates requires a system restart and terminates all active conferences. When you install or remove a certificate, the change is made to the certificate store immediately, but the system can’t implement the change until it restarts and reads the changed certificate store.

You are not required to restart and apply a change immediately. You can perform multiple installs or removals before restarting and applying the changes. When you are finished making changes, you must select Restart to Apply Saved Changes to restart the system and finish your update. Ensure there are no active conferences before you restart the system.

To install a signed certificate that identifies the RealPresence DMA system

1. When you receive your certificate(s), return to Admin > Server > Certificates.

2. In the Actions list, select Add Certificates.

3. In the Add Certificates dialog, do one of the following:

   - If you have a PFX, P7B, or single certificate file, click Upload certificate, enter the password (if any) for the file, and browse to the file or enter the path and file name.
If you have PEM-format text, copy the certificate text, click **Paste certificate**, and paste it into the text box below. You can paste multiple PEM certificates one after the other.

4. Click **OK**.

5. To verify that the new signed certificate has replaced the default self-signed certificate:
   a. In the list of certificates, once again select the **Server SSL** certificate.
   b. In the **Actions** list, select **Display Details**.
      The **Certificate Details** dialog appears.
   c. Confirm from the information under **Issued To** and **Issued By** that the self-signed default certificate has been replaced by your signed public certificate from the certificate authority.
   d. Click **OK** to close the dialog.

6. Click **Restart to Apply Saved Changes**, and when asked to confirm that you want to restart the system so that certificate changes can take effect, click **OK**.

### Removing Certificates

Installing or removing certificates requires a system restart and terminates all active conferences.

When you install or remove a certificate, the change is made to the certificate store immediately, but the system can’t implement the change until it restarts and reads the changed certificate store.

You are not required to restart and apply a change immediately. You can perform multiple installs or removals before restarting and applying the changes. When you are finished making changes, you must select **Restart to Apply Saved Changes** to restart the system and finish your update. Ensure there are no active conferences before you restart the system.

There are two kinds of certificate removal:

- Removing the certificate of a Trusted Root CA so that the system no longer trusts certificates signed by that certificate authority.
- Removing the signed certificate currently in use so that the system reverts to using the default self-signed certificate. Removing a signed certificate will not remove the certificate of the Trusted Root CA that signed it, or any intermediate certificates provided by that certificate authority.

This section includes the following topics:

- **Remove a Trusted Root CA’s Certificate**
- **Remove a Signed Certificate**

### Remove a Trusted Root CA’s Certificate

You can remove the certificate of a Trusted Root CA so that the system no longer trusts certificates signed by that certificate authority.

**To remove a Trusted Root CA’s certificate**

1. Go to **Admin > Server > Certificates**.
2. In the certificates list, select the certificate you want to delete.
3. In the **Actions** list, select **Display Details** and confirm that you’ve selected the correct certificate. Then click **OK**.
4 In the Actions list, select Delete Certificate.
5 When asked to confirm, click Yes.
   A dialog informs you that the certificate has been deleted.
6 Click OK.
7 Click Restart to Apply Saved Changes, and when asked to confirm that you want to restart the system so that certificate changes can take effect, click OK.

Remove a Signed Certificate

If you remove a signed certificate, the system reverts to the default self-signed certificate. Removing a signed certificate will not remove the certificate of the Trusted Root CA that signed it, or any intermediate certificates provided by that certificate authority.

Removing a signed certificate also removes the certificate of the Trusted Root CA that signed it, along with any intermediate certificates provided by that certificate authority.

To remove a signed certificate and revert to the default self-signed certificate

1 Go to Certificates.
2 In the Actions list, select Revert to Default Certificate.
3 When asked to confirm, click Yes.
   A dialog informs you that the system has reverted to a self-signed certificate.
4 Click OK.
5 Click Restart to Apply Saved Changes, and when asked to confirm that you want to restart the system so that certificate changes can take effect, click OK.
6 After the system restarts, log back in, return to Admin > Server > Certificates, and verify that the system has reverted to the default self-signed certificate:
   a In the list of certificates, select the Server SSL certificate.
   b In the Actions list, select Display Details.
      The Certificate Details dialog appears.
   c Confirm from the information under Issued To and Issued By that the default self-signed certificate has replaced the CA-signed certificate.
   d Click OK to close the dialog.
History Retention Settings

The Polycom® RealPresence® DMA® system is pre-configured with the number of history records of various types to retain. When the retention limit for a record type is reached, the system purges a specific number of the oldest records of that type.

The following table shows the retention limit for each record type and how many are purged at a time when the retention limit is reached. The values specified are for each cluster, not the total for the entire supercluster.

<table>
<thead>
<tr>
<th>Record Type</th>
<th>Retention Limit</th>
<th>Number of Records Purged When Limit Is Reached</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration history</td>
<td>505,000</td>
<td>5,000</td>
</tr>
<tr>
<td>Registration signaling</td>
<td>2,000,000</td>
<td>20,000</td>
</tr>
<tr>
<td>Call history</td>
<td>505,000</td>
<td>5,000</td>
</tr>
<tr>
<td>Call signaling history</td>
<td>12,625,000</td>
<td>125,000</td>
</tr>
<tr>
<td>Conference history</td>
<td>202,000</td>
<td>2,000</td>
</tr>
<tr>
<td>CDR export history</td>
<td>11,000</td>
<td>1,000</td>
</tr>
</tbody>
</table>

The History Retention Settings are supercluster-wide (the clusters are not independently configured).

Configure History Record Retention

You can specify whether to retain registration history records, and if so, whether to include registration keep-alive messages. You can also specify how many repeated low-value signaling records to retain.

Only users with the Auditor role can configure history retention settings.

To configure history record retention:

1. Log into the system as a user with the Auditor role and go to Admin > History Retention Settings.
2 Specify whether to record registration history, and if so, whether to include keep-alive messages.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable recording of registration history</td>
<td>Enables the system to retain Call Server registration records.</td>
</tr>
<tr>
<td>Include keep-alive messages in registration history</td>
<td>If selected, the Call Server history includes the keep-alive messages sent by registered endpoints and the Call Server's responses. Selecting this option significantly increases the number of Call Server registration records per period of time.</td>
</tr>
<tr>
<td>Number of repeated low-value signaling event records to retain</td>
<td>The number of less-important signaling messages (such as INFO messages about in-call status) to retain for a given call (from 0 to 10; default is 3). Once the limit is reached, subsequent messages of that type are processed, but not recorded in the call signaling history.</td>
</tr>
</tbody>
</table>

3 Specify how many low-value signaling records to retain.

4 Click **Update**.

5 Click **OK**.
Superclustering

The following topics describe the Polycom® RealPresence® DMA® system’s superclustering capability.

- About Superclustering
- Verify DNS FQDN Resolution
- View Details for RealPresence DMA Systems
- Create or Join a Supercluster
- Organize Territories and Assign Responsibilities
- Busy Out a Cluster
- Stop Using a Cluster
- Start Using a Cluster
- Remove a Cluster From a Supercluster

About Superclustering

Two Polycom RealPresence DMA systems can be configured as a co-located two-server cluster to enhance the reliability of the systems by providing redundancy. To provide even greater reliability, geographic redundancy, and improved network traffic management, multiple Polycom RealPresence DMA systems (either single-server or two-server systems) in distributed locations can be combined into a supercluster.

A supercluster is a set of up to 10 Polycom RealPresence DMA clusters that are geographically dispersed, but still centrally managed. The clusters in a supercluster are all peers. There is no “master” or “primary” cluster. All have local copies of the same data store, which is kept consistent via replication.

The common data store enables all of the superclustered RealPresence DMA systems to share data, including users, groups, conference rooms, services, site topology, dial plans, bandwidth management, endpoint registrations, usage reporting, status monitoring, Conference Manager configuration, Call Server configuration, and integrations. Sharing and replicating data also enables any cluster in the supercluster to configure or reconfigure the shared data.

Up to three clusters in a supercluster can function as Conference Managers, hosting conference rooms and managing pools of MCUs.

To use superclustering, you must have at least one DNS server. The host names (virtual and physical) of every cluster in the supercluster must be resolvable by all the other clusters. Each physical host name, physical IP address, and virtual host name must have A/AAAA records on your DNS server(s).

In addition to a DNS server, you must have at least one Network Time Protocol (NTP) server.
Verify DNS FQDN Resolution

Prior to creating a supercluster, you should verify that DNS can resolve all FQDNs of all clusters that will become part of the supercluster.

To verify DNS FQDN resolution for a cluster:
1. Go to Admin > Troubleshooting Utilities > Ping.
2. Ping the FQDNs (virtual and physical) of each cluster that will be part of the supercluster.

View Details for RealPresence DMA Systems

The DMAs list includes information about RealPresence DMA clusters. If the system you are logged in to is not (and has not been) part of a supercluster, the list contains only that system.

To view details for RealPresence DMA systems
1. Go to Integrations > DMAs.
2. View the following details about the RealPresence DMA systems on your network.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Indicates whether the cluster is superclustered and whether it is in service. Some clusters may be part of a supercluster but not currently be in service.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Virtual host name of the cluster’s management interface.</td>
</tr>
<tr>
<td>Model</td>
<td>Type of system. Currently, only RealPresence DMA systems may join a supercluster.</td>
</tr>
<tr>
<td>Version</td>
<td>Software version of the system.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Virtual IP address of the cluster’s management interface.</td>
</tr>
</tbody>
</table>

Create or Join a Supercluster

You can create or join a supercluster on the DMAs page.

To create a new supercluster, you must log in to a standalone cluster and invite a different standalone cluster to join the supercluster. Be sure to log in to the cluster that has the data and configuration you want to preserve as that data becomes the shared supercluster data store. After the cluster you invite accepts the invitation, both systems become clusters in the new supercluster. The system you invited to join has its local data store largely replaced by a copy of the data store from the system you are logged in to.

Note: All of the clusters in a supercluster must run compatible software versions. Patch releases of the same major version are usually compatible, but major version upgrades will not be compatible. If you plan to form a supercluster, upgrade each RealPresence DMA system to the latest version before doing so.
For example, if a cluster is integrated with your Polycom RealPresence Resource Manager system, log in to that cluster and invite other clusters to join the cluster you are logged in to. The site topology and user-to-device association data from the Polycom RealPresence Resource Manager system will be replicated throughout the supercluster.

When you invite a system to join a supercluster, active calls will continue uninterrupted on the system from which you send an invitation to join. However, all active calls will be terminated on the system you invite to join the supercluster.

**To create or join a supercluster:**

1. Go to **Integrations > DMAs**.
2. Under **ACTIONS**, click **Invite to Join Supercluster**.
3. Complete the fields as described in the following table.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name or IP address</td>
<td>The host name or IP address of the system you invite to join the supercluster. We strongly recommend specifying the FQDN of the virtual management interface for the cluster invited to join. You may specify an IP address; however, the virtual and physical host names of every cluster in the supercluster must be resolvable by all the other clusters. In a split network configuration, the host names are associated with the management network interface.</td>
</tr>
<tr>
<td>User name</td>
<td>An administrator login name for the cluster you invite to join.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for the administrator login.</td>
</tr>
</tbody>
</table>

4. Click **OK**.

   A prompt warns you that the invited system will restart and its local data will be overwritten.

5. Click **Yes** to confirm.

   The cluster you are logged in to connects to the cluster you invited to join and establishes the supercluster. The invited cluster obtains supercluster-wide configuration and data (this can take some time depending on the size of the data set). The system informs you when the process is complete and the invited cluster is ready to restart.

6. Click **OK**.

   You may need to restart your browser or clear your browser cache in order to log back into the system.

7. Log in to the system that joined the supercluster and verify that the **Supercluster Status** pane of the **Dashboard** shows the correct number of clusters.

8. Go to **Integrations > DMAs** and verify that the status of each RealPresence DMA cluster is **In service**.

9. Reassign territory responsibilities as needed.
Organize Territories and Assign Responsibilities

In a supercluster, the responsibility for most of the RealPresence DMA system’s functionality, including Active Directory and Exchange integration, device registration, call handling, and conference room (VMR) hosting, is assigned among the clusters using site topology territories. You can assign a set of responsibilities to each territory, and you can assign a primary cluster and a backup cluster for each territory. When the primary cluster is online, it controls the territory and carries out all of the responsibilities belonging to the territory. When the primary cluster is offline, the backup cluster assumes control of the territory and carries out all of the territory’s responsibilities.

A maximum of three territories can host conference rooms.

A standalone (not superclustered) RealPresence DMA system has a single default territory for which it is the primary cluster, without backup. When this cluster joins a supercluster, it still has the same single default territory, is still the primary cluster for the default territory, and still has no backup cluster. Essentially, one cluster is responsible for everything, and the others do nothing. Therefore, immediately after forming a new supercluster, you need to organize and create territories and assign functional responsibilities to those territories.

To organize territories and assign responsibilities to clusters:

1. Create your site topology data if you have not already done so, or integrate with a Polycom RealPresence Resource Manager system to obtain the data.

2. Organize your sites into territories that best distribute responsibilities and workload among the clusters of your supercluster. For example, with a five-cluster supercluster, do one of the following:
   - Create four territories, assign a primary cluster for each, and assign the fifth cluster as backup for all four.
   - Create five territories, assign a primary cluster for each, and make each cluster the backup for one of the other territories.
   - Use some hybrid of the preceding options that best suits your enterprise network’s distribution of sites, users, and traffic.

3. Create the territories, assign their functional responsibilities, and assign primary and backup clusters.

**Note:** If you have integrated with a Polycom RealPresence Resource Manager system, site topology data comes from that system and cannot be edited in the RealPresence DMA system. You must create the territories you need in the RealPresence Resource Manager system.

Busy Out a Cluster

When you Busy Out a selected cluster, you slowly decrease the use of the selected cluster:

- Existing calls and conferences on the selected cluster continue, but no new conferences are allowed to start. New calls are allowed to start only if they are associated with existing conferences. Registrations are rejected, except for endpoints currently involved in calls. The cluster ceases to manage bandwidth.
- Territories for which the selected cluster has primary responsibility and a different cluster has backup responsibility are transferred to the backup cluster.
• Registrations are seamlessly transferred to the backup cluster (for endpoints that support this). Bandwidth usage data for ongoing calls is seamlessly transferred to the backup cluster.

**To busy out a cluster**

1. Go to **Integrations > DMAs**.
2. Select the cluster to busy out and click **Busy Out**.
3. Click **OK** to confirm that you want to busy out the cluster.

**Stop Using a Cluster**

When you **Stop Using** a selected cluster, you take the cluster immediately out of service. This creates the following results:

• Existing calls and conferences on the selected cluster are disconnected. No new calls or conferences are allowed to start. All registrations are rejected. The cluster ceases to manage bandwidth.
• Territories for which the selected cluster has primary responsibility and a different cluster has backup responsibility are transferred to the backup cluster.
• Registrations are seamlessly transferred to the backup cluster (for endpoints that support this). Bandwidth usage data for ongoing calls is seamlessly transferred to the backup cluster.

**To stop using a cluster**

1. Go to **Integrations > DMAs**.
2. Select the cluster to stop using and click **Stop Using**.
3. Click **OK** to confirm that you want to stop using the cluster.

**Start Using a Cluster**

When you **Start Using** a cluster, you put the selected cluster back into service:

• New calls and conferences are allowed to start. The cluster begins bandwidth management.
• The cluster assumes control of any territories for which it has primary responsibility, or for which it has backup responsibility and the primary cluster is offline.
• For territories for which the restarted cluster is the primary, existing calls and conferences on the backup cluster continue, but no new conferences are allowed to start. New calls are allowed to start only if they are associated with existing conferences. The backup cluster ceases to manage bandwidth.
• Registrations are seamlessly transferred to the restarted primary cluster, where supported by the endpoint. Bandwidth usage data for ongoing calls is seamlessly transferred to the restarted primary cluster.

**To start using a cluster**

1. Go to **Integrations > DMAs**.
2. Select the cluster to start using and click **Start Using**.
3. Click **OK** to confirm that you want to start using the cluster.
Remove a Cluster From a Supercluster

You can remove a cluster from the supercluster, which re-initializes it as a new stand-alone cluster. It retains the data and configuration from the supercluster (including site topology), but that data is no longer synchronized to the common data store. If the cluster you plan to remove is responsible for any territories (as primary or backup), you must first reassign those territories.

**Note:** There is no mechanism for shutting down an entire supercluster. If you want to shut down all clusters in a supercluster, you must shut down and restart one cluster at a time.

To remove a cluster from a supercluster

1. Go to Integrations > DMAs.
2. Select the cluster to remove and click **Remove From Supercluster**.
3. Click **OK** to confirm that you want to remove the cluster from the supercluster.
External Device Configuration

This section provides an introduction to configuring external devices for use with the Polycom® RealPresence® DMA® system. It includes:

- External H.323 Gatekeepers
- External SIP Peers
- External H.323 Session Border Controllers
- External Skype for Business Systems
External H.323 Gatekeepers

When an enterprise has multiple neighbored gatekeepers, each gatekeeper manages its own H.323 zone. When a call originates in one gatekeeper zone and that zone’s gatekeeper is unable to resolve the dialed address, it forwards the call to the appropriate neighbor gatekeeper(s) for resolution.

Defining External H.323 Gatekeepers is a supercluster-wide configuration. A Polycom RealPresence DMA supercluster can manage multiple locations as a single H.323 zone, with the clusters acting as a single virtual gatekeeper. This allows the gatekeeper function to be geographically distributed, but managed centrally. A Polycom RealPresence DMA supercluster may eliminate the need for multiple zones and neighbor gatekeepers.

View External Gatekeepers

You can view a list of any external gatekeepers that you have integrated with your Polycom RealPresence DMA system.

To view the external gatekeepers:

» Go to Integrations > External H.323 Gatekeepers.

The following table describes the fields in the list.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the neighbored gatekeeper.</td>
</tr>
<tr>
<td>Description</td>
<td>Brief description of the gatekeeper.</td>
</tr>
<tr>
<td>Address</td>
<td>Host name or IP address of the gatekeeper.</td>
</tr>
<tr>
<td>Prefix Range</td>
<td>The dial string prefix(es) assigned to this neighbor gatekeeper.</td>
</tr>
<tr>
<td></td>
<td>If your dial plan uses the Dial services by prefix dial rule (in the default dial plan) to route calls to services, all dial strings beginning with an assigned prefix are forwarded to this gatekeeper for resolution.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Indicates whether the system is using the neighbor gatekeeper.</td>
</tr>
</tbody>
</table>

Add an External Gatekeeper

You can add an external gatekeeper to your system. This is a supercluster-wide configuration.
To add an external gatekeeper:
1. Go to Integrations > External H.323 Gatekeepers.
2. In the Actions list, click Add.
3. Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Check this box to enable the external gatekeeper you add. Clear this check box to stop using an external gatekeeper without deleting it.</td>
</tr>
<tr>
<td>Name</td>
<td>Gatekeeper name.</td>
</tr>
<tr>
<td>Description</td>
<td>The text description of the external gatekeeper.</td>
</tr>
<tr>
<td>Address</td>
<td>Host name or IP address of the gatekeeper.</td>
</tr>
<tr>
<td>RAS port</td>
<td>The RAS (Registration, Admission and Status) channel port number. Leave set to 1719 unless you know the gatekeeper is using a non-standard port number.</td>
</tr>
<tr>
<td>Prefix range</td>
<td>The dial string prefix or prefix range for which the external gatekeeper is responsible. Enter a single prefix (44), a range of prefixes (44-47), multiple prefixes separated by commas (44,46), or a combination (41, 44-47, 49). If your dial plan uses the Dial services by prefix dial rule (in the default dial plan) to route calls to services, all dial strings beginning with an assigned prefix are forwarded to this gatekeeper for resolution. If your dial plan instead uses a rule that you create to apply the Resolve to external gatekeeper action, there is no need to specify a prefix.</td>
</tr>
<tr>
<td>Strip prefix</td>
<td>If selected, the system strips the prefix when a call that includes a prefix is routed to this gatekeeper.</td>
</tr>
<tr>
<td>Prefer routed</td>
<td>If selected (the default), the system forces all calls to this gatekeeper to routed mode. This setting must be enabled to avoid interoperability issues with Polycom CMA and Avaya gatekeepers, and possibly others as well.</td>
</tr>
<tr>
<td>Authentication Mode</td>
<td>In this section, you can configure the system to send its H.235 credentials when it sends address resolution requests to the external gatekeeper.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Clearing this check box lets you stop sending H.235 credentials to the external gatekeeper without deleting them.</td>
</tr>
<tr>
<td>Name</td>
<td>The H.235 name of the Polycom RealPresence DMA system.</td>
</tr>
<tr>
<td>Password</td>
<td>The H.235 password for the Polycom RealPresence DMA system.</td>
</tr>
<tr>
<td>Algorithm</td>
<td>Select the encryption algorithm for H.235 authentication.</td>
</tr>
<tr>
<td>Send Test LRQ</td>
<td>Click to test the configuration by sending an LRQ message to the external gatekeeper.</td>
</tr>
</tbody>
</table>
Edit an External Gatekeeper

You can edit the configuration of an existing external gatekeeper as needed.

To edit an external gatekeeper:

1. Go to Integrations > External H.323 Gatekeepers.
2. Select the gatekeeper of interest and click Edit.
3. Revise the fields described in the following table as needed:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Gatekeeper</td>
<td>Clearing this check box lets you stop using an external gatekeeper without deleting it.</td>
</tr>
<tr>
<td>Name</td>
<td>Gatekeeper name.</td>
</tr>
<tr>
<td>Description</td>
<td>The text description displayed in the External Gatekeepers list.</td>
</tr>
<tr>
<td>Address</td>
<td>Host name or IP address of the gatekeeper.</td>
</tr>
<tr>
<td>RAS port</td>
<td>The RAS (Registration, Admission and Status) channel port number. Leave set to 1719 unless you know the gatekeeper is using a non-standard port number.</td>
</tr>
<tr>
<td>Prefix range</td>
<td>The dial string prefix or prefix range for which the external gatekeeper is responsible. Enter a single prefix (44), a range of prefixes (44-47), multiple prefixes separated by commas (44,46), or a combination (41, 44-47, 49). If your dial plan uses the Dial services by prefix dial rule (in the default dial plan) to route calls to services, all dial strings beginning with an assigned prefix are forwarded to this gatekeeper for resolution. If your dial plan instead uses a rule that you create to apply the Resolve to external gatekeeper action, there is no need to specify a prefix.</td>
</tr>
</tbody>
</table>
Add an External Gatekeeper With Both an IPv4 and IPv6 Address

When adding a neighbor gatekeeper, you can specify only one IP address. In an IPv4 plus IPv6 environment, to add a neighbor gatekeeper that has both an IPv4 and an IPv6 address, do the following:

- Add the neighbor gatekeeper using its IPv4 address.
- Add the neighbor gatekeeper a second time using its IPv6 address.
- Add one **Resolve to external gatekeeper** dial rule that specifies the neighbor gatekeeper’s IPv4 address entry (and no other gatekeepers).
- Add another **Resolve to external gatekeeper** dial rule that specifies the neighbor gatekeeper’s IPv6 address entry (and no other gatekeepers).

Requests from endpoints with IPv4 addresses will be forwarded to the gatekeeper’s IPv4 address, and requests from endpoints with IPv6 addresses will be forwarded to the gatekeeper’s IPv6 address.

---

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strip prefix</td>
<td>If selected, the system strips the prefix when a call that includes a prefix is routed to this gatekeeper.</td>
</tr>
<tr>
<td>Prefer routed</td>
<td>If selected (the default), the system forces all calls to this gatekeeper to routed mode.  This setting must be enabled to avoid interoperability issues with Polycom CMA and Avaya gatekeepers, and possibly others as well.</td>
</tr>
<tr>
<td>Authentication Mode</td>
<td>In this section, you can configure the system to send its H.235 credentials when it sends address resolution requests to that gatekeeper.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Clearing this check box lets you stop sending H.235 credentials to the external gatekeeper without deleting them.</td>
</tr>
<tr>
<td>Name</td>
<td>The H.235 name of the Polycom RealPresence DMA system.</td>
</tr>
<tr>
<td>Password</td>
<td>The H.235 password for the Polycom RealPresence DMA system.</td>
</tr>
<tr>
<td>Algorithm</td>
<td>Select the encryption algorithm for H.235 authentication.</td>
</tr>
<tr>
<td>Send Test LRQ</td>
<td>Click to test the configuration by sending an LRQ message to the external gatekeeper.</td>
</tr>
<tr>
<td>Postliminary</td>
<td>A postliminary is an executable script, written in the Javascript language, that defines dial string transformations to be applied before querying the external gatekeeper.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Lets you turn a postliminary on or off without deleting it.</td>
</tr>
<tr>
<td>Script</td>
<td>Type (or paste) the postliminary script you want to apply.</td>
</tr>
<tr>
<td>Debug this script</td>
<td>Click to verify the behavior of the script by opening the <strong>Script Debugging</strong> screen and then testing the script with different variables.</td>
</tr>
</tbody>
</table>
External SIP Peers

In a Polycom RealPresence DMA system, you can add or remove SIP servers or devices from a list of SIP peers to which the system can route calls and from which it may receive calls.

Defining External SIP Peers is a supercluster-wide configuration. A Polycom RealPresence DMA system supercluster can provide proxy service for any or all domains in the enterprise. This allows the SIP function to be distributed, but managed centrally and may reduce the need for external SIP peer servers, other than SIP session border controllers (SBCs). SIP SBCs to be reached by prefix-based dialing need to be added as External SIP Peers.

SBCs to be reached by a dial rule using the Resolve to external address or Resolve to IP address action are configured on a per-site basis.

For most configurations, SBCs should be configured on a per-site basis, so that calls to endpoints outside the enterprise network are routed to the SBC for the originating site.

Multiple External SIP Peers

The RealPresence DMA system can use multiple SIP peers to resolve dial strings. If a SIP peer experiences an outage, it is marked as unresponsive, and the RealPresence DMA system stops using it until it becomes responsive again. If you add multiple SIP peers to the system, you can configure how the system selects which SIP peer to use to resolve dial strings by using a dial rule with the Resolve to external SIP peer action.

When you configure a dial rule that uses the Resolve to external SIP peer action, you can choose which of two selection policies the system uses to resolve dial strings to SIP peers. If you select All in parallel (forking), the system tries all SIP peers simultaneously. If you select Weighted round-robin, you can assign each SIP peer a weight, with a higher weight giving a SIP peer higher priority, and the system tries each SIP peer sequentially according to the SIP peer’s assigned weight. You can change the weight for each SIP peer as necessary. Unresponsive SIP peers are considered only when there are no responsive peers that can complete the call.

SIP Peer Availability and Third-Party Network Devices

The RealPresence DMA system periodically uses SIP OPTIONS messages to verify connectivity with SIP peers. If a SIP peer fails to respond or responds with a specified set of status codes, the system removes that SIP peer from service. In some situations, a third-party device can respond on behalf of the SIP peer. If the RealPresence DMA system receives any other status code when the queried SIP peer is experiencing an outage, that SIP peer could incorrectly be marked as healthy.

Because of this, it is possible for a SIP peer’s service status to enter a “flapping” state. In this scenario, the RealPresence DMA system attempts to use the incorrectly marked SIP peer, but when the SIP peer fails to respond, the RealPresence DMA system removes the SIP peer from service. However, the RealPresence
DMA system receives a non-specified status code response for the next availability query, so puts the SIP peer back in service.

**View External SIP Peers**

The RealPresence DMA system displays a list of External SIP Peers and some of the configuration details for each peer. You can view the list for reference.

**To view external SIP peers:**

» Go to Integrations > External SIP Peers.

The following table describes the fields in the list of External SIP Peers.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the external SIP peer.</td>
</tr>
<tr>
<td><strong>UDP TCP TLS</strong></td>
<td>Provides a visual responsiveness status of each SIP peer for the UDP, TCP, and TLS protocols, depending on what <strong>Transport type</strong> the system is configured to use when contacting this SIP peer. If the <strong>Transport type</strong> is set to <strong>Auto Detect</strong>, the system may use multiple transport types and may display an icon indicating responsiveness for each type it uses. Responsiveness status for each SIP peer in the list is updated every ten seconds by default.</td>
</tr>
<tr>
<td>Description</td>
<td>Brief description of the external SIP peer.</td>
</tr>
<tr>
<td>Next Hop Address</td>
<td>Fully qualified domain name (FQDN) or IP address of the external SIP peer.</td>
</tr>
<tr>
<td>Prefix Range</td>
<td>The dial string prefix(es) assigned to this external SIP peer. If your dial plan uses the <strong>Dial services by prefix</strong> dial rule (in the default dial plan) to route calls to services, all dial strings beginning with an assigned prefix are forwarded to this SIP peer for resolution.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Indicates whether the system is using the external SIP peer.</td>
</tr>
<tr>
<td><strong>External Registrations</strong></td>
<td>Indicates whether the system is registered with the external SIP peer so that it can route calls to it. Displays “Active” if there are any <strong>External Registrations</strong> defined for this SIP peer that are enabled.</td>
</tr>
</tbody>
</table>

**Add an External SIP Peer**

You can add one or more external SIP peers to your RealPresence DMA system.

**To add an external SIP peer:**

1. Go to Integrations > External SIP Peers.
2. In the Actions list, click Add.
3 Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>External SIP Peers</strong></td>
<td></td>
</tr>
<tr>
<td>Enabled</td>
<td>Select the check box to enable use of this external SIP peer. Clear the check box lets to stop using the external SIP peer without deleting it.</td>
</tr>
<tr>
<td>Name</td>
<td>Peer name or number. Must be unique among SIP peers.</td>
</tr>
<tr>
<td>Description</td>
<td>The text description of the external SIP peer.</td>
</tr>
<tr>
<td>Type</td>
<td>For a Microsoft Office Communications Server, Lync Server or Skype for Business Server, select Microsoft. Otherwise, select Other. Selecting Microsoft implicitly adds the Destination network value to the Domain List (if not already there) and automatically selects the Postliminary settings that are correct for most deployments in Microsoft environments, but you can modify them if necessary. Note: Selecting Microsoft enables the Skype Integration tab.</td>
</tr>
<tr>
<td>Next hop address</td>
<td>Fully qualified domain name (FQDN), host name, or IP address of the SIP peer. Spaces after the name are not allowed. If you specify a domain/host name, the system routes calls to this peer by using DNS to resolve the address. The DNS server that the system uses must contain the required records (NAPTR, SRV, and/or A/AAAA). Note: If you are configuring a Lync 2013 or Skype for Business SIP Peer, the Next hop address should be the FQDN or IP address of the Lync or Skype front-end pool, not an individual Lync or Skype server within a pool.</td>
</tr>
<tr>
<td>Destination network</td>
<td>Host name, FQDN, or network domain label of the SIP peer, with or without port and URL parameters. If specified, this value by default replaces the non-user portion of a URL (after the @ symbol) of the To header and Request-URI for forwarded messages, and the Request-URI for REGISTER messages. If Type is set to Microsoft, this field is required and is used for the peer’s domain. Note: This field is used as the SIP domain for Polycom RealConnect™ conferences.</td>
</tr>
<tr>
<td>Port</td>
<td>The SIP signaling port number. Defaults to the standard UDP/TCP port, 5060. If the peer server is using a different port number, specify it. Note: For a Lync or Skype for Business SIP peer, the port should be 5061. If left blank, the system determines the port via DNS.</td>
</tr>
<tr>
<td>Transport type</td>
<td>The transport protocol to use when contacting this SIP peer. The default is TCP. Auto detect tells the system to select the protocol using DNS as specified in RFC 3263, and is not valid if Next hop address is a numeric IP address instead of a host/domain name.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Use route header</td>
<td>Add a route header with the peer’s <strong>Next hop address</strong> value to the message. Applies to both forwarded messages and external REGISTER messages. If not selected, the only valid Request-URI configurations are those that use the peer's <strong>Next hop address</strong> value for the URI host. <strong>Note:</strong> Disable this option for Lync or Skype for Business SIP peers that will accept content sessions from Polycom RealPresence ContentConnect™ applications through the RealPresence DMA system.</td>
</tr>
<tr>
<td>Downgrade</td>
<td>If selected, and if this peer doesn’t support TLS, the system can change the Request-URI schema from sips to sip and route the call to this peer. If not selected, the system routes a TLS call to this peer only if this peer supports TLS.</td>
</tr>
</tbody>
</table>
| Prefix range          | The dial string prefix(es) assigned to this SIP peer. Enter a single prefix (44), a range of prefixes (44-47), or multiple prefixes separated by commas (44,46). If your dial plan uses the **Dial services by prefix** dial rule (in the default dial plan) to route calls to services, all dial strings beginning with an assigned prefix are forwarded to this SIP peer for resolution. If your dial plan instead uses a rule that you create to apply the **Resolve to external SIP peer** action, there is no need to specify a prefix. Otherwise, the system applies the **SIP Routing** settings of the originating site for calls to endpoints outside the enterprise network. **Note:** For a SIP peer, the dial string must either include the protocol or consist of only the prefix and user name (no @domain). For instance, if the SIP peer’s prefix is 123, the dial string for a call to alice@polycom.com must be one of the following:  
  sip:123alice@polycom.com  
  sips:123alice@polycom.com  
  123alice                                                                 |
| Strip prefix          | If selected, the system strips the prefix when a call that includes a prefix is routed to this peer.                                                                                                                                                                                                                                                               |
| Register externally   | Some external SIP peers require peers to register with them as an endpoint does, using a REGISTER message (also referred to as pilot registration). Select this option to enable the **External Registration** tab and configure the system to register with this external SIP peer, following the rules specified in RFC 3261.                                                                 |
| Supports SIP OPTIONS ping | If selected, the system sends SIP OPTIONS ping messages to the SIP peer to determine its responsiveness. See the **Service Config > Call Server Settings** page for configuration options related to SIP OPTIONS ping messages.                                                                                                  |
### Domain List
If your dial plan uses a rule to apply the Resolve to external SIP peer action, you can restrict calls to this SIP peer to specific domains by adding the authorized domains to this list.

If this list is empty, all domains can resolve to this peer.

**Note:** In some circumstances (depending on network topology and configuration), dialing loops can develop if you don't restrict SIP peers to specific domains.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add new domain</td>
<td>Enter a domain and click <strong>Add</strong> to add it to the list of authorized domains.</td>
</tr>
<tr>
<td>Authorized domains</td>
<td>List of administrative domains, contained in the dial string, for which calls are routed to this SIP peer. Leave this list empty to route any call that matches the rule to this SIP peer. Select a domain and click <strong>Remove</strong> to remove it from the list.</td>
</tr>
</tbody>
</table>

### Postliminary
If checked, the fields on this page are available and in effect. If unchecked, the fields are disabled and the original SIP signaling is passed unchanged to the SIP peer.

This field is unchecked by default if you select a **Type** of Microsoft when adding a SIP peer.

**Note:** Polycom recommends leaving postliminary scripts disabled for Microsoft SIP peers to ensure proper signaling operation with calls to external Lync or Skype for Business systems.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use output format</td>
<td>Enables dial string transformations using the To header options and Request-URI options below instead of a customized script.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The system generates a script that implements the settings made in this section. To see (and perhaps copy) the generated script, you can temporarily select <strong>Use customized script</strong>.</td>
</tr>
<tr>
<td></td>
<td>To help you learn how to write your own script, you can make different settings in this section and see how the generated script changes.</td>
</tr>
</tbody>
</table>

### To header options
Specify the format of the To header in messages sent to this peer.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy all parameters of original &quot;To&quot; headers</td>
<td>Copies any parameters included in the original To header to the To header sent to this peer. This setting applies to all format options.</td>
</tr>
</tbody>
</table>

### Format Template
Select a predefined format from the list, or select **Free Form Template** and define the format in the associated **Template** field.

### Request URI options
Specify the format of the Request-URI.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format Template</td>
<td>Select a predefined format from the list, or select <strong>Free Form Template</strong> and define the format in the associated <strong>Template</strong> field.</td>
</tr>
</tbody>
</table>
Use customized script

Enables you to write or paste an executable script in Javascript in the text box below. Using such a script enables you to more flexibly define dial string and message format transformations to be applied.

Type (or paste) the postliminary script you want to apply. Then click **Debug this Script** to test the script with different variables.

**Note:** When you change settings in the **Use output format** section, the system generates a script that implements those settings. Select this option to see (and perhaps copy) the generated script. The functions in the generated script return string values and accept string parameters.

**Authentication**

On this tab, you can configure SIP digest authentication for this SIP peer and add or edit authentication credentials.

SIP authentication must be enabled and configured in Device Authentication.

**Note:** The digest authentication settings for this peer are used only in conjunction with a dial rule specifying the **Resolve to external SIP peer** action. If another dial rule action, such as **Resolve to external address**, is applied to the call, there is no association to this peer and its authentication settings are not used.

**Outbound Authentication**

Select one:

- **Handle authentication** — When it receives a 401 (Unauthorized) response from this SIP peer, the Call Server presents its authentication credentials. If there are no authentication credentials for the specified realm, the response is passed back to the originating call leg.
- **Pass authentication** — When it receives a 401 response from this SIP peer, the Call Server passes it to the source of the request.

**Outbound Proxy Authentication**

Select one:

- **Handle proxy authentication** — When it receives a 407 (Proxy Authentication Required) response from this SIP peer, the Call Server presents its authentication credentials. If there are no authentication credentials for the specified realm, the response is passed back to the originating call leg.
- **Pass proxy authentication** — When it receives a 407 response from this SIP peer, the Call Server passes it to the source of the request.

**Inbound Authentication**

Determines if the RealPresence DMA system requires authentication credentials when an outbound call receives an inbound request.

Select one:

- **Always challenge peer** — inbound requests will be challenged for authentication credentials.
- **Never challenge peer** — inbound requests will not be challenged for authentication credentials.

When you enable SIP authentication for endpoints, it is not currently possible to define behavior regarding unauthenticated ports.

When you enable SIP authentication for both standard and custom ports and define an external SIP peer using the custom port, the system routes calls to the custom port. However, the Contact header in the outbound SIP INVITE message from the RealPresence DMA system contains port 5060. This causes the in-dialogue message to be rejected with a 401 response.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(table of authentication entries)</td>
<td>Lists the authentication credential entries defined for use with this SIP peer, showing the realm in which the entry is valid and the user name. Click <strong>Add</strong> to add authentication credentials. When choosing authentication credentials to present to this SIP peer, the Call Server looks first at the entries listed here. If there is none with the correct realm, it looks for an appropriate entry on the Device Authentication page.</td>
</tr>
<tr>
<td>Skype Integration</td>
<td>This tab contains fields necessary to integrate with a Lync 2013 or Skype for Business server, and is enabled when you select a <strong>Type</strong> of <strong>Microsoft</strong> on the <strong>External SIP Peers</strong> tab.</td>
</tr>
</tbody>
</table>
| Maximum Polycom conference contacts to publish | The maximum number of Polycom conference contacts that the RealPresence DMA system attempts to publish to this SIP peer.  
**Note:** If this field is set to the default value of 0, the **Lync pool to create/publish to** field on the **Service Config > Conference Manager Settings > Conference Settings** page remains blank.  
If this value is lower than the number of conference contacts configured for presence publishing, a system alert is raised.  
The maximum Polycom conference contacts to publish is 25,000. |
| Enable RealConnect™ conferences | Indicates that this Lync or Skype for Business SIP peer should be cascaded with Polycom MCUs for on-premises Polycom RealConnect™ conferences. If enabled, this SIP peer is used to resolve Lync or or Skype conference IDs.  
This option must be enabled for this SIP peer to appear in the **Available SIP peers** area in dial rules that use the **Resolve to Skype conference ID** action.  
**Note:** This option does not apply to RealConnect™ conferences with external Lync or Skype for Business systems. |
| Skype account URI             | The account ID the RealPresence DMA system should use when resolving Lync or Skype for Business conference IDs. Any user account on the Lync or Skype server can be used.  
This field is enabled when **Enable RealConnect™ conferences** is checked. |
| MCU pool order                | The MCU pool order this Lync or Skype for Business SIP peer uses for Polycom MCUs that provide Skype AVMCU cascade functionality. If you leave this option unchecked, the **Dial to on-premises RealConnect™ conference** dial rule will use the **MCU pool order** you selected for the rule in **Admin > Call Server > Dial Rules**.  
This field is enabled when **Enable RealConnect™ conferences** is checked. |
Edit an External SIP Peer

You can edit an existing external SIP peer when necessary.

To edit an external SIP peer:

1. Go to Integrations > External SIP Peers.
2. Select the SIP peer to revise and click Edit.
3. Revise the following fields as needed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CsTrustedApplication</td>
<td>The GRUU value that the system should use when communicating with Lync or Skype for Business clients that connect to VMR conferences.</td>
</tr>
<tr>
<td>ServiceGruu</td>
<td>When enabled, the RealPresence DMA system includes the text field value in the signaling it sends to Lync or or Skype for Business clients that have joined VMR conferences. This identifies the RealPresence DMA system as a trusted application when communicating with these clients. Enabling this option can prevent calls from Lync or Skype for Business clients to VMRs that are many hours in length from disconnecting unexpectedly. See the Polycom Unified Communications for Microsoft Environments - Solution Deployment Guide for information on obtaining the GRUU value to populate this field.</td>
</tr>
</tbody>
</table>

| External Registrations | Lists any outbound registration configurations associated with this SIP peer and lets you add, edit, or delete registrations. Multiple registrations may be associated with a SIP peer. |

4. Click OK.

Field

<table>
<thead>
<tr>
<th>Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Enabled</td>
<td>Clearing this check box lets you stop using an external SIP peer without deleting it.</td>
</tr>
<tr>
<td>Name</td>
<td>Peer name or number. Must be unique among SIP peers.</td>
</tr>
<tr>
<td>Description</td>
<td>The text description displayed in the External SIP Peer list.</td>
</tr>
<tr>
<td>Type</td>
<td>For a Microsoft Office Communications Server, Lync Server or Skype for Business Server, select Microsoft. Otherwise, select Other. Selecting Microsoft implicitly adds the Destination network value to the Domain List (if not already there) and automatically selects the Postliminary settings that are correct for most deployments in Microsoft environments, but you can modify them if necessary. Note: Selecting Microsoft enables the Skype Integration tab.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Next hop address</td>
<td>Fully qualified domain name (FQDN), host name, or IP address of the SIP peer. Spaces after the name are not allowed. If you specify a domain/host name, the system routes calls to this peer by using DNS to resolve the address. The DNS server that the system uses must contain the required records (NAPTR, SRV, and/or A/AAAA).  <strong>Note:</strong> If you are configuring a Lync 2013 or Skype for Business SIP Peer, the <strong>Next hop address</strong> should be the FQDN or IP address of the Lync or Skype front-end pool, not an individual Lync or Skype server within a pool.</td>
</tr>
<tr>
<td>Destination network</td>
<td>Host name, FQDN, or network domain label of the SIP peer, with or without port and URL parameters. If specified, this value by default replaces the non-user portion of a URL (after the @ symbol) of the To header and Request-URI for forwarded messages, and the Request-URI for REGISTER messages. If <strong>Type</strong> is set to Microsoft, this field is required and is used for the peer’s domain.  <strong>Note:</strong> This field is used as the SIP domain for Polycom RealConnect™ conferences.</td>
</tr>
<tr>
<td>Port</td>
<td>The SIP signaling port number. Defaults to the standard UDP/TCP port, 5060. If the peer server is using a different port number, specify it.  <strong>Note:</strong> For a Lync or Skype for Business SIP peer, the port should be 5061. If left blank, the system determines the port via DNS.</td>
</tr>
<tr>
<td>Transport type</td>
<td>The transport protocol to use when contacting this SIP peer. The default is TCP.  <strong>Auto detect</strong> tells the system to select the protocol using DNS as specified in RFC 3263, and is not valid if <strong>Next hop address</strong> is a numeric IP address instead of a host/domain name.</td>
</tr>
<tr>
<td>Use route header</td>
<td>Add a route header with the peer’s <strong>Next hop address</strong> value to the message. Applies to both forwarded messages and external REGISTER messages. If not selected, the only valid Request-URI configurations are those that use the peer’s <strong>Next hop address</strong> value for the URI host.  <strong>Note:</strong> Disable this option for Lync or Skype for Business SIP peers that will accept content sessions from Polycom RealPresence ContentConnect™ applications through the RealPresence DMA system.</td>
</tr>
<tr>
<td>Downgrade</td>
<td>If selected, and if this peer doesn’t support TLS, the system can change the Request-URI schema from sips to sip and route the call to this peer. If not selected, the system routes a TLS call to this peer only if this peer supports TLS.</td>
</tr>
</tbody>
</table>
External SIP Peers

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Prefix range</strong></td>
<td>The dial string prefix(es) assigned to this SIP peer. Enter a single prefix (44), a range of prefixes (44-47), or multiple prefixes separated by commas (44,46)</td>
</tr>
<tr>
<td></td>
<td>If your dial plan uses the <strong>Dial services by prefix</strong> dial rule (in the default dial plan) to route calls to services, all dial strings beginning with an assigned prefix are forwarded to this SIP peer for resolution.</td>
</tr>
<tr>
<td></td>
<td>If your dial plan instead uses a rule that you create to apply the <strong>Resolve to external SIP peer</strong> action, there is no need to specify a prefix.</td>
</tr>
<tr>
<td></td>
<td>Otherwise, the system applies the <strong>SIP Routing</strong> settings of the originating site for calls to endpoints outside the enterprise network.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For a SIP peer, the dial string must either include the protocol or consist of only the prefix and user name (no @domain). For instance, if the SIP peer's prefix is 123, the dial string for a call to <a href="mailto:alice@polycom.com">alice@polycom.com</a> must be one of the following:</td>
</tr>
<tr>
<td></td>
<td>sip:<a href="mailto:123alice@polycom.com">123alice@polycom.com</a></td>
</tr>
<tr>
<td></td>
<td>sips:<a href="mailto:123alice@polycom.com">123alice@polycom.com</a></td>
</tr>
<tr>
<td></td>
<td>123alice</td>
</tr>
<tr>
<td><strong>Strip prefix</strong></td>
<td>If selected, the system strips the prefix when a call that includes a prefix is routed to this peer.</td>
</tr>
<tr>
<td><strong>Register externally</strong></td>
<td>Some external SIP peers require peers to register with them as an endpoint does, using a REGISTER message (also referred to as <em>pilot registration</em>). Select this option to enable the <strong>External Registration</strong> tab and configure the system to register with this external SIP peer, following the rules specified in RFC 3261.</td>
</tr>
<tr>
<td><strong>Supports SIP OPTIONS ping</strong></td>
<td>If selected, the system sends SIP OPTIONS ping messages to the SIP peer to determine its responsiveness. See the <strong>Service Config &gt; Call Server Settings</strong> page for configuration options related to SIP OPTIONS ping messages.</td>
</tr>
<tr>
<td><strong>Domain List</strong></td>
<td>If your dial plan uses a rule to apply the <strong>Resolve to external SIP peer</strong> action, you can restrict calls to this SIP peer to specific domains by adding the authorized domains to this list.</td>
</tr>
<tr>
<td></td>
<td>If this list is empty, all domains can resolve to this peer. <strong>Note:</strong> In some circumstances (depending on network topology and configuration), dialing loops can develop if you don't restrict SIP peers to specific domains.</td>
</tr>
<tr>
<td><strong>Add new domain</strong></td>
<td>Enter a domain and click <strong>Add</strong> to add it to the list of authorized domains.</td>
</tr>
<tr>
<td><strong>Authorized domains</strong></td>
<td>List of administrative domains, contained in the dial string, for which calls are routed to this SIP peer. Leave this list empty to route any call that matches the rule to this SIP peer. Select a domain and click <strong>Remove</strong> to remove it from the list.</td>
</tr>
</tbody>
</table>
### External SIP Peers

#### Postliminary

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enabled                | If checked, the fields on this page are available and in effect. If unchecked, the fields are disabled and the original SIP signaling is passed unchanged to the SIP peer.  
This field is unchecked by default if you select a **Type** of Microsoft when adding a SIP peer.  
**Note:** Polycom recommends leaving postliminary scripts disabled for Microsoft SIP peers to ensure proper signaling operation with calls to external Lync or Skype for Business systems. |

#### Use output format

Enables dial string transformations using the **To header options** and **Request-URI options** below instead of a customized script.  
**Note:** The system generates a script that implements the settings made in this section. To see (and perhaps copy) the generated script, you can temporarily select **Use customized script**.  
To help you learn how to write your own script, you can make different settings in this section and see how the generated script changes.

#### To header options

Specify the format of the To header in messages sent to this peer.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy all parameters of original “To” headers</td>
<td>Copies any parameters included in the original To header to the To header sent to this peer. This setting applies to all format options.</td>
</tr>
</tbody>
</table>

#### Request URI options

Specify the format of the Request-URI.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Format Template              | Select a predefined format from the list, or select **Free Form Template** and define the format in the associated **Template** field.  
The predefined formats in the list and the variables you use in the **Template** field are described in **SIP Peer Postliminary Output Format Options**. |

#### Use customized script

Enables you to write or paste an executable script in Javascript in the text box below. Using such a script enables you to more flexibly define dial string and message format transformations to be applied.  
Type (or paste) the postliminary script you want to apply. Then click **Debug this Script** to test the script with different variables.  
**Note:** When you change settings in the **Use output format** section, the system generates a script that implements those settings. Select this option to see (and perhaps copy) the generated script. The functions in the generated script return string values and accept string parameters.
On this tab, you can configure SIP digest authentication for this SIP peer and add or edit authentication credentials. SIP authentication must be enabled and configured in Device Authentication. **Note:** The digest authentication settings for this peer are used only in conjunction with a dial rule specifying the **Resolve to external SIP peer** action. If another dial rule action, such as **Resolve to external address**, is applied to the call, there is no association to this peer and its authentication settings are not used.

**Outbound Authentication**
Select one:
- **Handle authentication** — When it receives a 401 (Unauthorized) response from this SIP peer, the Call Server presents its authentication credentials. If there are no authentication credentials for the specified realm, the response is passed back to the originating call leg.
- **Pass authentication** — When it receives a 401 response from this SIP peer, the Call Server passes it to the source of the request.

**Outbound Proxy Authentication**
Select one:
- **Handle proxy authentication** — When it receives a 407 (Proxy Authentication Required) response from this SIP peer, the Call Server presents its authentication credentials. If there are no authentication credentials for the specified realm, the response is passed back to the originating call leg.
- **Pass proxy authentication** — When it receives a 407 response from this SIP peer, the Call Server passes it to the source of the request.

**Inbound Authentication**
Determines if the RealPresence DMA system requires authentication credentials when an outbound call receives an inbound request. Select one:
- **Always challenge peer** — inbound requests will be challenged for authentication credentials.
- **Never challenge peer** — inbound requests will not be challenged for authentication credentials.

When you enable SIP authentication for endpoints, it is not currently possible to define behavior regarding unauthenticated ports.

When you enable SIP authentication for both standard and custom ports and define an external SIP peer using the custom port, the system routes calls to the custom port. However, the Contact header in the outbound SIP INVITE message from the RealPresence DMA system contains port 5060. This causes the in-dialogue message to be rejected with a 401 response.

**Table of authentication entries**
Lists the authentication credential entries defined for use with this SIP peer, showing the realm in which the entry is valid and the user name. Click **Add** to add authentication credentials.

When choosing authentication credentials to present to this SIP peer, the Call Server looks first at the entries listed here. If there is none with the correct realm, it looks for an appropriate entry on the **Device Authentication** page.

**Skype Integration**
This tab contains fields necessary to integrate with a Lync 2013 or Skype for Business server, and is enabled when you select a **Type** of **Microsoft** on the **External SIP Peers** tab.
External SIP Peers

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Polycom conference</td>
<td>The maximum number of Polycom conference contacts that the RealPresence DMA system attempts to publish to this SIP peer.</td>
</tr>
<tr>
<td>contacts to publish</td>
<td><strong>Note:</strong> If this field is set to the default value of 0, the <strong>Lync pool to create/publish to</strong> field on the <strong>Service Config &gt; Conference Manager Settings &gt; Conference Settings</strong> page remains blank.</td>
</tr>
<tr>
<td></td>
<td>If this value is lower than the number of conference contacts configured for presence publishing, a system alert is raised.</td>
</tr>
<tr>
<td></td>
<td>The maximum Polycom conference contacts to publish is 25,000.</td>
</tr>
<tr>
<td>Enable RealConnect™ conferences</td>
<td>Indicates that this Lync or Skype for Business SIP peer should be cascaded with Polycom MCUs for on-premises Polycom RealConnect™ conferences. If enabled, this SIP peer is used to resolve Lync or or Skype conference IDs.</td>
</tr>
<tr>
<td></td>
<td>This option must be enabled for this SIP peer to appear in the <strong>Available SIP peers</strong> area in dial rules that use the <strong>Resolve to Skype conference ID</strong> action.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This option does not apply to RealConnect™ conferences with external Lync or Skype for Business systems.</td>
</tr>
<tr>
<td>Skype account URI</td>
<td>The account ID the RealPresence DMA system should use when resolving Lync or Skype for Business conference IDs. Any user account on the Lync or Skype server can be used.</td>
</tr>
<tr>
<td></td>
<td>This field is enabled when <strong>Enable RealConnect™ conferences</strong> is checked.</td>
</tr>
<tr>
<td>MCU pool order</td>
<td>The MCU pool order this Lync or Skype for Business SIP peer uses for Polycom MCUs that provide Skype AV/MCU cascade functionality. If you leave this option unchecked, the <strong>Dial to on-premises RealConnect™ conference</strong> dial rule will use the <strong>MCU pool order</strong> you selected for the rule in <strong>Admin &gt; Call Server &gt; Dial Rules</strong>.</td>
</tr>
<tr>
<td></td>
<td>This field is enabled when <strong>Enable RealConnect™ conferences</strong> is checked.</td>
</tr>
<tr>
<td>CsTrustedApplication</td>
<td>The GRUU value that the system should use when communicating with Lync or Skype for Business clients that connect to VMR conferences.</td>
</tr>
<tr>
<td>ServiceGruu</td>
<td>When enabled, the RealPresence DMA system includes the text field value in the signaling it sends to Lync or or Skype for Business clients that have joined VMR conferences. This identifies the RealPresence DMA system as a trusted application when communicating with these clients.</td>
</tr>
<tr>
<td></td>
<td>Enabling this option can prevent calls from Lync or Skype for Business clients to VMRs that are many hours in length from disconnecting unexpectedly. See the <strong>Polycom Unified Communications for Microsoft Environments - Solution Deployment Guide</strong> for information on obtaining the GRUU value to populate this field.</td>
</tr>
<tr>
<td>External Registrations</td>
<td>Lists any outbound registration configurations associated with this SIP peer and lets you add, edit, or delete registrations. Multiple registrations may be associated with a SIP peer.</td>
</tr>
</tbody>
</table>

4 Click **OK** to save the changes.

**SIP Peer Postliminary Output Format Options**

This section includes the following information to help with the postliminary settings for an external SIP peer:
● To Header Format Options
● Request-URI Header Format Options
● Free Form Template Variables
● To Header and Request-URI Header Examples

### To Header Format Options

The settings available on the Format list for the To header are described below. If a user is present in the URI, the user is always preserved except when Free Form Template is selected.

**Use original request’s To** — The To header from the original request is copied and used as is. Equivalent to template:

"#otdisplay#" <#otscheme#:otuser#@#othost#>

**No Display, use original request’s To** — The To header from the original request is copied and used. If a display parameter is present, it’s removed. Equivalent to template:

<#otscheme#:otuser#@#othost#>

**With Display, use peer’s next hop address as host** — URI’s host is replaced with the Next hop address value for this peer. No other changes are made. Equivalent to template:

"#otdisplay#" <#pscheme#:otuser#@#phost#>

**No Display, use original request’s URL host** — The To header from the original request is copied, the URI is replaced with the host/IP portion of the original request’s Request-URI. If a display parameter is present, it’s removed. Equivalent to template:

<#pscheme#:otuser#@#orhost#>

**No Display, use peer’s Destination Network or next hop address** — Uses the Destination network value if specified, otherwise the peer’s Next hop address value. If a display parameter is present, it’s removed. Equivalent to template:

<#pscheme#:otuser#@#pnetORphost#>

**Default To header for Microsoft.** — Equivalent to template:

"#otdisplay#" <sip:#otuser#@#pnetORphost#>

**Free Form Template** — Format defined in associated Template field is used without further modification.

### Request-URI Header Format Options

The settings available on the Format list for the Request-URI header are described below (RR= requires route header):

**Use original request’s URI (RR)** — The original request’s URI is copied and moved. Equivalent to template:

#orscheme#:oruser#@#orhost#

**No user, original request’s host (RR)** — The user in the original, if any, is removed, but the original host is used. Equivalent to template:

#orscheme#:orhost#
No user, configured peer’s next hop address as host — The user in the original, if any, is removed, and the host is replaced with the Next hop address value for this peer. Equivalent to template:

#pscheme#:#phost#

Original user, configured peer’s next hop address as host — The user in the original is copied, but the host is replaced with the Next hop address value for this peer. Equivalent to template:

#pscheme#:#oruser#@#phost#

Note: If the peer’s transport type is configured as TLS, this setting makes the Request-URI scheme sips even if the original Request-URI’s scheme was sip. Some SIP peers, such as the Cisco SBC, won’t accept sips in the Request-URI if other headers contain sip. If this problem exists, change Format to Free Form Template and in the Template field, change #pscheme# to #orscheme#.

Use user as host (RR) — Uses the user in the original, if specified, as the host value, otherwise the host value is used as is. Equivalent to template:

#orscheme#:#oruser#  
(but if no original user is present, the host value is used as is)

No user, configured peer’s Destination Network or next hop address — Uses the Destination network value if specified, otherwise the peer’s Next hop address value. Equivalent to template:

#pscheme#:#pnetORphost#

Original user, configured peer’s Destination Network or next hop address — Uses the user in the original, if specified, but replaces the host with the Destination network value, if specified, or the peer’s Next hop address value. Equivalent to template:

#pscheme#:#otuser#@#pnetORphost#

Default Request-URI for Microsoft — Equivalent to template:

sip:#oruser#@#pnetORphost#:#pport#;transport=#ptransport#

Request-URI for Microsoft without CSS — Equivalent to template:

sip:#phost#:#pport#;transport=#ptransport#

Free Form Template — Format defined in associated Template field is used without further modification.

### Free Form Template Variables

In the Template fields on the Postliminary tab, and when specifying a Request-URI or other headers for outbound registration, you can use the variables in the following table entered as #variable name# (case insensitive). The system replaces the variables with the corresponding values as shown below.

You can also use these variables (without # delimiters) in a customized script.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>otdisplay</td>
<td>Original To header’s display name.</td>
</tr>
<tr>
<td>otuser</td>
<td>User portion of the original request's To header URL field.</td>
</tr>
<tr>
<td>othost</td>
<td>Host/IP portion of the original request's To header URL field.</td>
</tr>
</tbody>
</table>
In addition to the variables, you can enter any values acceptable for the Request-URI or To header. For the Request-URI, the contents of the Template field specify only the URI portion of the full Request line. Depending on network configuration, a Route header may be required. For the To header, the contents of the Template field specify the complete header except for the header name (“To”). The @ symbol is always removed if no user is present in the result.

**To Header and Request-URI Header Examples**

The following tables show some examples of To header and Request-URI header transformations using free form template variables.

<table>
<thead>
<tr>
<th>Original To Header</th>
<th>Template</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>sip:user@host</td>
<td>#otscheme#:atest</td>
<td>sip:atest</td>
</tr>
<tr>
<td>sip:user@host</td>
<td>#otscheme#:#otuser#@#othost#</td>
<td>sip:user@host</td>
</tr>
<tr>
<td>sip:host</td>
<td>#otscheme#:#otuser#@foo.bar</td>
<td>sip:foo.bar</td>
</tr>
<tr>
<td>sip:user@host</td>
<td>#otscheme#:#otuser#@foo.bar</td>
<td>sip:<a href="mailto:user@foo.bar">user@foo.bar</a></td>
</tr>
<tr>
<td>sip:host</td>
<td>sips:#otuser#@foo.bar</td>
<td>sips:foo.bar</td>
</tr>
<tr>
<td>sip:user@host</td>
<td>#otscheme#:#otuser#@#othost#</td>
<td>sip:user@toHeaderUrlHost</td>
</tr>
</tbody>
</table>
Add an Authentication Credential Entry

You can add an authentication credential entry either for a specific external SIP peer or to the general list of outbound authentication credentials that the system uses if challenged by an external device.

To add an authentication credential entry

1. Go to Integrations > External SIP Peers.
2. In the Actions list, click Add.
3. In Add External SIP Peer, select Authentication.
4. Click Add to add an authentication entry.
5. Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Realm</td>
<td>Unique string that identifies the protection domain to which this set of credentials applies. Generally includes the host or domain name of the SIP peer. See RFC 2617 and RFC 3261.</td>
</tr>
<tr>
<td>User name</td>
<td>The user name to use for authentications in this realm.</td>
</tr>
<tr>
<td>Password</td>
<td>The password to use for authentications in this realm.</td>
</tr>
<tr>
<td>Confirm password</td>
<td></td>
</tr>
</tbody>
</table>

6. Click OK.

Edit an Authentication Credential Entry

You can edit an authentication credential entry either for a specific external SIP peer (see Edit an External SIP Peer) or from the general list of outbound credentials for the system.
To edit an authentication credential entry:

1. Go to Integrations > External SIP Peers.
2. Select the SIP peer of interest and click Edit.
3. In the Edit External SIP Peer dialog, select Authentication.
4. Select the authentication credential entry to revise and click Edit.
5. Edit the following fields as needed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Realm</td>
<td>Unique string that identifies the protection domain to which this set of credentials applies. Generally includes the host or domain name of the SIP peer. See RFC 2617 and RFC 3261.</td>
</tr>
<tr>
<td>User name</td>
<td>The user name to use for authentications in this realm.</td>
</tr>
<tr>
<td>Password Confirm password</td>
<td>The password to use for authentications in this realm.</td>
</tr>
</tbody>
</table>

6. Click OK.

Add an External Registration

Some external SIP peers require peers to register with them as an endpoint does, using a REGISTER message (also known as pilot registration). You can add external registration configurations that the RealPresence DMA system can use to register with the SIP peer that you are adding or editing.

To add an external registration

1. Go to Integrations > External SIP Peers.
2. In the Actions list, click Add.
3. In Add External SIP Peer, select External Registrations.
4. Click Add to add an external registration.
5. Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Clearing this check box lets you stop using this registration without deleting the registration information.</td>
</tr>
<tr>
<td>Address of record</td>
<td>The address of record with which the RealPresence DMA system registers (see registration rules in RFC 3261), such as: sip:<a href="mailto:1000@dma.polycom.com">1000@dma.polycom.com</a></td>
</tr>
<tr>
<td>Territory to perform registration</td>
<td>Responsibility for registering must be assigned to a territory, thus making the primary or backup RealPresence DMA cluster for the territory responsible, depending on which is active.</td>
</tr>
</tbody>
</table>
Click OK.

Edit an External Registration

You can edit external registration configurations that the RealPresence DMA system can use to register with the SIP peer that you are editing.

To edit an external registration

1. Go to Integrations > External SIP Peers.
2. Select the External Sip Peer to edit and in the Actions list, click Edit.
3. In Edit External SIP Peer, select External Registrations.
4. Select the external registration to revise and click Edit.
5. Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact address format</td>
<td>Select <strong>IP Address</strong> or <strong>DNS Name</strong> to specify that the contact header should use the virtual IP address or virtual DNS name of the cluster currently managing the territory. If the territory responsibility switches to the other cluster, it re-sends the registration using its IP address or DNS name. Select <strong>Free Form</strong> to specify that the contact header should use the FQDN you enter. The external SIP peer must be able to resolve this FQDN.</td>
</tr>
<tr>
<td>User name</td>
<td>The user name to use for the authentication credentials if the external peer challenges the registration request. <strong>Note:</strong> The authentication credentials specified here are specific to this SIP peer and are not tied to any other authentication configuration values.</td>
</tr>
<tr>
<td>Password</td>
<td>The password to use for the authentication credentials if the external peer challenges the registration request.</td>
</tr>
<tr>
<td>Confirm password</td>
<td></td>
</tr>
<tr>
<td>Request-URI</td>
<td>The Request-URI to include when registering with this SIP peer, specified using the Free Form Template Variables (#delimited). <strong>Note:</strong> Request-URI and other headers are available only when <strong>Use route header</strong> is enabled in the External SIP Peers section.</td>
</tr>
<tr>
<td>Other headers</td>
<td>Additional headers to include when registering with this SIP peer. Click Add to add a header. In the Add Header dialog, specify the header name and value(s), using the Free Form Template Variables (#delimited). Click Edit or Delete to edit or delete the selected header.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Clearing this check box lets you stop using this registration without deleting the registration information.</td>
</tr>
<tr>
<td>Address of record</td>
<td>The address of record with which the RealPresence DMA system registers (see registration rules in RFC 3261), such as: sip:<a href="mailto:1000@dma.polycom.com">1000@dma.polycom.com</a></td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Territory to perform registration | Responsibility for registering must be assigned to a territory, thus making the primary or backup RealPresence DMA cluster for the territory responsible, depending on which is active.

Contact address format | Select **IP Address** or **DNS Name** to specify that the contact header should use the virtual IP address or virtual DNS name of the cluster currently managing the territory. If the territory responsibility switches to the other cluster, it re-sends the registration using its IP address or DNS name. Select **Free Form** to specify that the contact header should use the FQDN you enter. The external SIP peer must be able to resolve this FQDN.

User name | The user name to use for the authentication credentials if the external peer challenges the registration request. **Note:** The authentication credentials specified here are specific to this SIP peer and are not tied to any other authentication configuration values.

Password | The password to use for the authentication credentials if the external peer challenges the registration request.

Confirm password | The password to use for the authentication credentials if the external peer challenges the registration request.

Request-URI | The Request-URI to include when registering with this SIP peer, specified using the Free Form Template Variables (#delimited). **Note:** Request-URI and other headers are available only when **Use route header** is enabled in the **External SIP Peers** section.

---

6 Click **OK**.
External H.323 Session Border Controllers

In an H.323 environment, H.323 session border controllers (SBCs) regulate access across the firewall. You can add or remove H.323 SBCs that the system can use to reach endpoints outside the enterprise network by prefix-based dialing. When you add, edit, or delete H.323 SBCs, the configurations are supercluster-wide.

H.323 SBCs that are added to the External H.323 SBC page are reached by prefix-based dialing.

SBCs to be reached by a dial rule using the Resolve to IP address action (rule 6 of the default dial plan) are configured on a per-site basis.

In general, H.323 SBCs should be configured on a per-site basis, so that calls to endpoints outside the enterprise network are routed to the SBC assigned to the originating site.

In general, you should configure H.323 SBCs on a per-site basis, so that calls to endpoints outside the enterprise network are routed to the SBC assigned to the originating site. Session border controllers to be reached by a dial rule using the Resolve to IP address action are configured on a per-site basis.

There are three reasons to configure an H.323 SBC on the External H.323 SBC page:

- To create a prefix service that allows dialing through the specific SBC by prefix. An SBC configured on this page must have a prefix or prefix range assigned to it and can only be reached by dialing its prefix(es).
- To define a postliminary script to be applied when dialing through the specific SBC.
- For bandwidth management.

The Polycom RealPresence DMA system is capable of performing call admission control (CAC) while processing an LRQ from a neighbor gatekeeper. This allows the system to reject the call for resource or policy reasons early in the setup process (in response to the LRQ), rather than waiting until later in the call setup.

In order to perform early CAC, the Polycom RealPresence DMA system must know the caller’s media address, which is not provided in the LRQ and is unknowable for an ordinary gatekeeper. If the gatekeeper is also an SBC, however, it proxies the media. The Polycom RealPresence DMA system can assume that its media address is the same as its signaling address, and proceed with early CAC. The Polycom RealPresence DMA system performs early CAC only in response to LRQs received from SBCs configured on the External H.323 SBC page.

View External H.323 SBCs

You can view a list of external H.323 SBCs that you have added to your RealPresence DMA system.
To view a list of external H.323 SBCs:

» Go to Integrations > External H.323 SBCs.

The following table describes the fields in the list.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the SBC.</td>
</tr>
<tr>
<td>Description</td>
<td>Brief description of the SBC.</td>
</tr>
<tr>
<td>Address</td>
<td>Host name or IP address of the SBC.</td>
</tr>
<tr>
<td>Prefix Range</td>
<td>The dial string prefix(es) assigned to this SBC.</td>
</tr>
<tr>
<td></td>
<td>If your dial plan uses the Dial services by prefix dial rule (in the default dial plan) to route calls to services, all dial strings beginning with an assigned prefix are forwarded to this SBC for resolution.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Indicates whether the system is using the SBC.</td>
</tr>
</tbody>
</table>

Add an External H.323 SBC

You can add an external H.323 SBC to your system.

To add an external H.323 SBC:

1. Go to Integration > External H.323 SBCs.
2. In the Actions list, click Add.

The following table describes the fields in the Add External H.323 SBC dialog.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>External H.323 SBC</td>
<td>Clearing this check box lets you stop using an external SBC without deleting it.</td>
</tr>
<tr>
<td>Enabled</td>
<td>SBC unit name.</td>
</tr>
<tr>
<td>Name</td>
<td>The text description displayed in the External H.323 SBC list.</td>
</tr>
<tr>
<td>Description</td>
<td>Host name or IP address of the SBC.</td>
</tr>
<tr>
<td>Address</td>
<td>The SBC’s port number. Leave set to 1720 unless you know the unit is using a non-standard port number.</td>
</tr>
<tr>
<td>Port</td>
<td>The dial string prefix or prefix range assigned to this SBC. Required. Enter a single prefix (44), a range of prefixes (44-47), or multiple prefixes separated by commas (44,46)</td>
</tr>
<tr>
<td>Prefix range</td>
<td>The Dial services by prefix dial rule in the default dial plan routes calls to the assigned prefix(es) to this SBC for resolution.</td>
</tr>
</tbody>
</table>
Edit an External H.323 SBC

You can edit an H.323 SBC that exists on your system.

Only H.323 SBCs are added to the External H.323 SBC page. SIP SBCs are configured as SIP peers (see External SIP Peers) and/or on a per-site basis.

SBCs to be reached by a dial rule using the Resolve to IP address action are configured on a per-site basis (see Edit a Site).

In general, H.323 SBCs should be configured on a per-site basis, so that calls to endpoints outside the enterprise network are routed to the SBC assigned to the originating site.

To edit an external H.323 SBC:

1. Go to Integration > External H.323 SBCs.
2. In the Actions list, click Edit.
   
   The following table describes the fields in the Edit External H.323 SBC dialog.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strip prefix</td>
<td>If selected, the system strips the prefix when a call that includes a prefix is routed to this SBC.</td>
</tr>
<tr>
<td>Postliminary</td>
<td>A postliminary is an executable script, written in the Javascript language, that defines dial string transformations to be applied before querying the SBC.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Lets you turn a postliminary on or off without deleting it.</td>
</tr>
<tr>
<td>Script</td>
<td>Type (or paste) the postliminary script you want to apply. Then click Debug this Script to open the Test Preliminary and Postliminary Scripts and test the script with various variables.</td>
</tr>
</tbody>
</table>

3. Click OK.
<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix range</td>
<td>The dial string prefix or prefix range assigned to this SBC. Required. Enter a single prefix (44), a range of prefixes (44-47), or multiple prefixes separated by commas (44,46) The Dial services by prefix dial rule in the default dial plan routes calls to the assigned prefix(es) to this SBC for resolution.</td>
</tr>
<tr>
<td>Strip prefix</td>
<td>If selected, the system strips the prefix when a call that includes a prefix is routed to this SBC.</td>
</tr>
<tr>
<td>Postliminary</td>
<td>A postliminary is an executable script, written in the Javascript language, that defines dial string transformations to be applied before querying the SBC.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Lets you turn a postliminary on or off without deleting it.</td>
</tr>
<tr>
<td>Script</td>
<td>Type (or paste) the postliminary script you want to apply. Then click Debug this Script to open the Test Preliminary and Postliminary Scripts and test the script with various variables.</td>
</tr>
</tbody>
</table>

3 Click OK.
External Skype for Business Systems

When you define an external Skype for Business system, your local Polycom infrastructure gains the ability to connect to a remote Skype deployment and start or join Polycom RealConnect™ conferences on that system. An external Skype system is a Skype deployment located at a remote site that has a federated relationship with your Skype deployment.

Microsoft Skype systems configured as external SIP peers enable RealConnect™ conferencing for Skype deployments within your network. External Skype systems extend that capability to Skype deployments outside of your network.

When the RealPresence DMA system routes a call to an external Skype system, it uses the prefix defined for the external Skype system to determine which external Skype system to use. It then selects a Polycom MCU to host the conference and contact the external Skype system’s Conference Auto Attendant (CAA) service. The RealPresence DMA system selects an Active Directory callback contact and passes it to the selected MCU. The Skype AVMCU calls the local MCU to establish a cascade link, joining the local MCU to the conference. The MCU uses the callback contact to communicate with the local and external Skype systems, ensuring that the call is forwarded properly from the remote AVMCU to the local MCU.

Due to the nature of interacting with the external Skype system’s CAA service, there may be a delay of up to 20 seconds before participants are added to the conference they dialed.

Participants can connect to RealConnect™ conferences hosted on external Skype systems in three ways:

- **Dialing manually, using the dial string pattern**
  
  `<Prefix><Skype_Conference_ID>@<DMA_hostname><DMA_Domain>`

- **Dialing a Virtual Entry Queue (VEQ) and entering**
  
  `<prefix><Skype_Conference_ID>`

- **Click-to-Connect, using the RealConnect™ Proxy service (contact Polycom Professional Services for more information)**

Participants using endpoints not registered to the RealPresence DMA system where the external Skype system is deployed need to manually dial these conferences using the full dial string pattern above. To make dialing simpler, you can create an address book entry on these endpoints that dials a VEQ that is associated with a unique external Skype system. The participant then dials the address book entry and is prompted for the RealConnect™ conference ID. For more information on associating a VEQ with a unique external Skype system, see Shared Number Dialing.

View External Skype for Business Systems

You can view information about the external Skype systems that have a federated relationship with your Skype deployment.
To view external Skype systems:

» Go to Integrations > External Skype Systems.

The following table describes the fields on the External Skype Systems page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name for the external Skype system.</td>
</tr>
<tr>
<td>Description</td>
<td>An optional description of the external Skype system.</td>
</tr>
<tr>
<td>Prefix</td>
<td>An optional prefix that identifies this external Skype system to the RealPresence DMA system.</td>
</tr>
<tr>
<td>CAA Dial-in SIP URI</td>
<td>The SIP address of the Conference Auto Attendant (CAA) for the external Skype system.</td>
</tr>
<tr>
<td>Conference template</td>
<td>The conference template MCUs use when establishing RealConnect™ conferences with this external Skype system.</td>
</tr>
<tr>
<td>MCU pool order</td>
<td>The MCU pool order MCUs use when establishing RealConnect™ conferences with this external Skype system.</td>
</tr>
<tr>
<td>MCU Selection</td>
<td>The method for the RealPresence DMA system to use when it selects MCUs from MCU pool orders:</td>
</tr>
<tr>
<td></td>
<td>Prefer MCU in first MCU pool ensures that the DMA system always routes the call to the first available MCU in the first MCU pool. If no MCU is available, the system searches the second MCU pool for an available MCU, and so on.</td>
</tr>
<tr>
<td></td>
<td>Prefer MCU in first caller's site matches the MCU chosen for the call with the site that the first caller's endpoint belongs to.</td>
</tr>
<tr>
<td>Virtual Entry Queues</td>
<td>A list of VEQs that specify this external Skype system as a Unique external Skype system. Configured on the Service Config &gt; Conference Manager Settings &gt; Shared Number Dialing page.</td>
</tr>
</tbody>
</table>

Add an External Skype System

Before you add an external Skype system, ensure that Active Directory integration is enabled and at least one Microsoft external SIP peer is defined in the RealPresence DMA system.

To configure an external Skype system, you must complete the following tasks:

- Ensure the required certificates are installed (See the Polycom Unified Communications for Microsoft Environments - Solution Deployment Guide).
- On your Active Directory server, configure Active Directory accounts for use as callback contacts (See the Polycom Unified Communications for Microsoft Environments - Solution Deployment Guide).
- Add an external Skype system configuration to the RealPresence DMA system.
- Choose an Active Directory callback contact OU on the Integrations > Microsoft Active Directory page.
- Configure a dial rule with the action Resolve to Skype Conference ID by Conference Auto Attendant.
You must create all Active Directory callback contacts within a single OU, and ensure that there are enough callback contacts in the OU for the cluster to use under heavy conferencing loads (one callback contact is used for each call to an external Skype system). There can be up to 2400 concurrent RealConnect™ conferences hosted on external Skype systems.

To add an external Skype system:

1. Go to the Integrations > External Skype Systems.
2. In the Actions list, click Add.
3. In the Add External Skype System dialog, complete the editable fields, described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name for the external Skype system (up to 64 characters).</td>
</tr>
<tr>
<td>Description</td>
<td>An optional description of the external Skype system (up to 128 characters).</td>
</tr>
<tr>
<td>Prefix</td>
<td>An optional prefix that identifies this external Skype system to the RealPresence DMA system (up to 8 characters). Callers add this prefix to the beginning of a dial string to dial in to a conference on this specific external Skype system. When the system matches dial strings against prefixes, the longest match for that dial string is used. For example, if you define an external Skype system with the prefix ‘2’ and another with the prefix ‘22’, the dial string ‘225678’ results in a conference ID of ‘5678’. If you do not specify a prefix, when the system executes a dial rule that includes this external Skype system, all dial strings will match and no further dial rules will be run. <strong>Note:</strong> Prefixes defined for external Skype systems are not listed on the Service Config &gt; Dial Plan &gt; Prefix Service page. <strong>Note:</strong> No two external Skype systems can have the same prefix, and only one external Skype system can have a blank prefix.</td>
</tr>
<tr>
<td>CAA Dial-in SIP URI</td>
<td>The SIP address of the Conference Auto Attendant (CAA) for the external Skype system (up to 128 characters). The “sip:” URI scheme is required. <strong>Note:</strong> The RealPresence DMA system does not dial this SIP URI, but instead passes it to the MCU. Ensure the Polycom MCUs that are part of this solution are the correct version (8.6 or later) and can communicate with the external Skype system’s CAA.</td>
</tr>
<tr>
<td>Conference template</td>
<td>The conference template MCUs should use when establishing RealConnect™ conferences with this external Skype system.</td>
</tr>
<tr>
<td>MCU pool order</td>
<td>The MCU pool order MCUs should use when establishing RealConnect™ conferences with this external Skype system.</td>
</tr>
</tbody>
</table>
| MCU Selection          | The method for the RealPresence DMA system to use when it selects MCUs from MCU pool orders:  
**Prefer MCU in first MCU pool** ensures that the DMA system always routes the call to the first available MCU in the first MCU pool. If no MCU is available, the system searches the second MCU pool for an available MCU, and so on.  
**Prefer MCU in first caller’s site** matches the MCU chosen for the call with the site that the first caller’s endpoint belongs to. |
4 Click OK.

5 Go to Integrations > Microsoft Active Directory.

6 Enable the Callback contacts OU field and enter the path of a container that contains the callback contact accounts you configured earlier.

For information on how to configure callback contact accounts in Active Directory, see the Polycom Unified Communications for Microsoft Environments - Solution Deployment Guide.

7 Click OK.

8 Go to Service Config > Dial Plan > Dial Plans to configure the RealPresence DMA system to actively use this external Skype system for calls.

9 Do one of the following:
   - If a dial rule with the action Resolve to Skype Conference ID by Conference Auto Attendant exists, select it and click Edit in the Actions menu.
   - If a dial rule with this action does not exist, click Add to create one.

10 Ensure the dial rule is enabled.

11 Move this external Skype system from the Available external Skype systems box to the Selected external Skype systems box.

12 Click OK.

Edit an External Skype System

In some circumstances you may need to update the configuration of an external Skype system (for example, if the remote site changes the external Skype system’s settings).

To edit an external Skype for Business system:

1 Go to the Integrations > External Skype Systems.

2 In the Actions list, click Add.

3 In the Edit External Skype System screen, make any changes necessary to the editable fields, described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name for the external Skype for Business system (up to 64 characters).</td>
</tr>
<tr>
<td>Description</td>
<td>An optional description of the external Skype for Business system (up to 128 characters).</td>
</tr>
<tr>
<td>Prefix</td>
<td>An optional prefix that identifies this external Skype for Business system to the RealPresence DMA system (up to 8 characters). Callers add this prefix to the beginning of a dial string to dial a conference on this specific external Skype for Business system. If you do not specify a prefix, when the system executes a dial rule that includes this external Skype for Business system, all dial strings will match and no further dial rules are run. <strong>Note:</strong> No two external Skype for Business systems can have the same prefix, and only one external Skype for Business system can have a blank prefix.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
CA A Dial-in SIP URI | The SIP address of the Conference Auto Attendant (CAA) for the external Skype for Business system (up to 128 characters). The “sip:” protocol prefix is required. **Note:** The RealPresence DMA system does not dial this SIP URI, but instead passes it to the MCU. Ensure the Polycom MCUs that are part of this solution are the correct version (8.6 or later) and can communicate with the external Skype for Business system’s CAA.
Conference template | The conference template MCUs should use when establishing RealConnect™ conferences with this external Skype for Business system.
MCU pool order | The MCU pool order MCUs should use when establishing RealConnect™ conferences with this external Skype for Business system.
MCU Selection | The method for the RealPresence DMA system to use when it selects MCUs from MCU pool orders: **Prefer MCU in first MCU pool** ensures that the DMA system always routes the call to the first available MCU in the first MCU pool. If no MCU is available, the system searches the second MCU pool for an available MCU, and so on. **Prefer MCU in first caller’s site** matches the MCU chosen for the call with the site that the first caller’s endpoint belongs to.

4 Click **OK**.
MCU Management

This section provides an introduction to managing MCUs with the Polycom® RealPresence® DMA® system. It includes:

- MCU Management
- MCUs
- MCU Pools and Pool Orders
MCU Management

The Polycom RealPresence DMA system can integrate with Multipoint Control Units (MCUs) to enable multipoint video conferencing. A multipoint video conference is one in which multiple endpoints are connected, with all participants able to see and hear each other. The endpoints connect to an MCU, which processes the audio and video from each endpoint and sends the conference audio and video streams back to them.

You must organize MCUs configured as conferencing resources into one or more MCU pools (logical groupings of media servers). Then, you can define one or more MCU pool orders that specify the order of preference in which the RealPresence DMA system uses MCU pools.

Every conference room (virtual meeting room, or VMR) is associated with an MCU pool order. The pool(s) to which an MCU belongs, and the pool order(s) to which a pool belongs, are used to determine which MCU is used to host a conference.

Configuring a Polycom MCU for use with the RealPresence DMA System

You must configure a Polycom MCU to be compatible with the management functions of the RealPresence DMA system before adding it to the system.

For more detailed instructions on configuring a Polycom MCU, please see the MCU product documentation.

Configure Compatible Security Settings

In enhanced security mode, the RealPresence DMA system uses only HTTPS for the conference control connection to MCUs, and you must configure your MCUs to accept encrypted connections. When unencrypted connections are used, the MCU login name and password are sent unencrypted over the network.

Configure User Connections

By default, a RealPresence Collaboration Server or RMX MCU allows up to 20 connections per user. We recommend not reducing this setting on the MCU (the MAX_NUMBER_OF_MANAGEMENT_SESSIONS_PER_USER system flag). If you have a RealPresence DMA supercluster with three Conference Manager clusters and a busy conferencing environment, we recommend increasing this value to 30.
**Disable Automatic Password Generation**

The Automatic Password Generation feature is not compatible with the RealPresence DMA system. On Polycom MCUs to be used with the RealPresence DMA system, disable this feature by setting the system flags NUMERIC_CONF_PASS_DEFAULT_LEN and NUMERIC_CHAIR_PASS_DEFAULT_LEN both to 0 (zero).

**Configure SIP Settings**

In a SIP signaling environment, in order for a Polycom RealPresence Collaboration Server or RMX MCU to register with the RealPresence DMA system’s Call Server, two system flags on the MCU must be set properly:

- Set the MS_ENVIRONMENT flag to NO.
- Make sure the SIP_REGISTERONLYONLY_ONCE flag is set to NO or is not present.

**Configuring a Cisco MCU for use with the Polycom® RealPresence® DMA® System**

You need to ensure that the settings on any supported Cisco MCU are compatible with the RealPresence DMA system.

**Disable Media Port Reservations**

The Polycom RealPresence DMA system supports the use of Cisco Codian 4200, 4500, and MSE 8000 series MCUs as conferencing resources, but their Media Port Reservation feature is not supported. This feature must be disabled on Cisco Codian MCUs.

**Using ISDN Gateways**

When a Polycom RealPresence Collaboration Server or RMX MCU functions as an ISDN gateway, each call through the gateway uses two ports, one for the ISDN side and one for the H.323 side. The ports used for gateway calls are not available for conferences, so gateway operations may significantly reduce the available conferencing resources.

**ISDN Gateway Selection Process**

When the dial string begins with a simplified ISDN gateway dialing prefix, the Polycom RealPresence DMA system chooses an ISDN gateway by applying the following steps:

1. Strip the ISDN gateway dialing prefix from the dial string, leaving the E.164 number.
2. From the in-service (not busied out or out of service) gateways, select the ones that have a profile with a matching or higher bit rate (higher bit rate can only be used for RealPresence Collaboration Server or RMX MCUs). If none, go to 3; otherwise, go to 4.
3. From the remaining gateways, select those with a profile bit rate lower than the requested bit rate. If none, reject the call.
4 From the remaining gateways, select those that match the country code and area code of the dialed number. If none, go to 5; otherwise, go to 6.

5 From the remaining gateways, select those that match the country code of the dialed number, if any.

6 From the remaining gateways, select those with a profile that has the closest bit rate. An exact match is preferred.

7 From the remaining gateways, select those that are in the same site as the calling endpoint, if any.

8 From the remaining gateways, select one using a round-robin method.

9 If the call fails because of no capacity on the selected gateway, select the next gateway left in 8. If none, start again at 2 (omitting the gateway that failed). If none left, reject the call.

10 If a gateway is successfully selected, assemble a dial string to send to the gateway as follows:
   `<direct dial-in prefix><session profile prefix><delimiter><E.1`

**Bandwidth Management**

For H.323 calls to a conference room (virtual meeting room, or VMR), the RealPresence DMA system can only do bandwidth management if the MCU is registered with it (in a supercluster, registered with any cluster). If the MCU is unregistered or registered to another gatekeeper (not part of the supercluster), the bandwidth for the call is not counted for bandwidth management, site statistics, or the network usage report.

For the RealPresence DMA system to assign an alternate gatekeeper to an MCU, the MCU must be in a territory that has a backup RealPresence DMA system assigned to it.
MCUs

The RealPresence DMA system is aware of all MCUs that have registered with the Call Server and any you have manually added. You can view a list of all MCUs known to the system. In a superclustered system, this list encompasses all MCUs throughout the supercluster and is the same on all clusters in the supercluster. It includes:

- MCUs that are available as a conferencing resource for the Polycom RealPresence DMA system's Conference Manager (enabled for conference rooms), but aren't registered with the Call Server. Up to 64 MCUs can be enabled for conference rooms (virtual meeting rooms, or VMRs).
- MCUs that are registered with the Polycom RealPresence DMA system's Call Server as standalone MCUs and/or ISDN gateways, but aren't available to the Conference Manager as conferencing resources.
- MCUs that are both registered with the Call Server and available to the Conference Manager as conferencing resources.

View the MCUs List

You can view a list of MCUs and gateways, or a combination of the two, that are available to the Polycom RealPresence DMA system. This allows you to view an MCU's connection status, the IP address, and additional details.

An MCU can appear in this list either because it registered with the Call Server or because it was manually added. If the MCU registered itself, it can be used as a standalone MCU. In order for the Conference Manager to use such an MCU as a conferencing resource, you must edit its details to enable it for conference rooms and provide the additional configuration information required.

To view the MCUs list:

1. Go to Integrations > MCUs.

The following table describes the fields in the MCUs list.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status and Alarm State</td>
<td>Connection and service status and alarm state of an MCU (hover over an icon to see the associated status message).</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the MCU.</td>
</tr>
<tr>
<td>Model</td>
<td>The type of MCU.</td>
</tr>
<tr>
<td>Version</td>
<td>The version of software on the MCU.</td>
</tr>
<tr>
<td>IP Addresses</td>
<td>The IP addresses for the MCU’s management interface (M) and signaling interface (S).</td>
</tr>
</tbody>
</table>
View MCU Details

You can view configuration details for any managed MCU.

To view MCU details:

1. Go to Integrations > MCUs to view the list of MCUs.
2. In the MCUs list, select the MCU of interest.
3. Under Actions, click View Details.

The screen lists configuration details for the selected MCU.

Add an MCU

You can add an MCU, gateway, or combination of the two to the pool of devices available to the Polycom RealPresence DMA system.

To add an MCU:

1. Go to Integrations > MCUs.
2. Under Actions, click Add.
3. Enter the MCU settings, as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MCU General Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Name for the MCU (up to 32 characters; must not include any of the following: , &quot; ; ? : = *).</td>
</tr>
<tr>
<td>Type</td>
<td>Lists the types of MCUs the system supports. Must be set to the correct MCU type in order for the RealPresence DMA system to be able to connect to it. For an MGC MCU, this must be set to Polycom MGC gateway, even if it is being used as a standalone MCU.</td>
</tr>
</tbody>
</table>
Integrate with conference manager

When checked, enables the MCU to be used as a conferencing resource for the RealPresence DMA system's Conference Manager.

**Caution:** Before adding an MCU to the RealPresence DMA system’s conferencing resources, make sure the MCU is not already a conferencing resource for an integrated RealPresence Resource Manager system. The RealPresence Resource Manager system must have exclusive use of any MCUs on which it directly schedules conferences. A Polycom MCU can be managed by the RealPresence Resource Manager system or the RealPresence DMA system, not both.

Management IP address

Host name or IP address for the RealPresence DMA system to log into the MCU to use it as a conferencing resource.

**Note:** Polycom MCUs don't include their management IP address in the Subject Alternate Name (SAN) field of the CSR (Certificate Signing Request), so their certificates identify them only by the Common Name (CN). Therefore if **Skip validation of certificates received while making outbound connections** is off in Security Settings, the MCU’s management interface must be identified by the name specified in the CN field (usually the FQDN), not by IP address.

Admin user ID

Administrative user ID with which the Polycom RealPresence DMA system can log into the MCU.

Password

Password for the administrative user ID.

CIF Video ports reserved for non-DMA use

The number of video ports on this MCU that are off-limits to the Polycom RealPresence DMA system.

Voice ports reserved for non-DMA use

The number of voice ports on this MCU that are off-limits to the Polycom RealPresence DMA system.

Cascade-for-size reserved CIF video ports

The number of video ports on this MCU to reserve for cascade links when a conference that has cascade-for-size enabled is created on this MCU.

Per-conference

For each cascade-for-size conference on this MCU, this number of video ports is subtracted from the number of video ports available for participants. These ports are instead reserved for cascade links.

Overall

The number of video ports reserved for cascade-for-size cascade links on this MCU (in addition to the Per-conference value).

**Direct Access Settings**

Enable Direct Access

Enables the MCU to be used as a directly addressed device, independent of whether the Conference Manager uses the MCU. When selected, the signaling addresses and ports for the MCU and the MCU's media addresses must be configured. If the setting **Integrate with conference manager** is selected on the **MCU General Settings** tab, the system will automatically populate these values when it accesses the MCU.

Signaling IP for H.323

The address that the MCU uses for H.323 signaling. If you specify the login information for the MCU, this field is optional (the system can get the address from the MCU). If not, and H.323 is enabled, this field is required.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signaling IP for SIP</td>
<td>The address that the MCU uses for SIP signaling. If you specify the login information for the MCU, this field is optional (the system can get the address from the MCU). If not, and SIP is enabled, this field is required.</td>
</tr>
<tr>
<td>Transport</td>
<td>The SIP transport type to use with this MCU. If the RealPresence DMA system's security settings do not allow unencrypted connections, this must be TLS.</td>
</tr>
<tr>
<td>Add Media IP Addresses</td>
<td>If you specify the login settings for the MCU, the system can get media addresses from the MCU. If not, enter an IP address for media streams and click <strong>Add</strong> to add it the list.</td>
</tr>
<tr>
<td>Remove Media IP Addresses</td>
<td>Select a media address and click <strong>Remove</strong> to delete it from the list.</td>
</tr>
<tr>
<td>Direct dial-in prefix</td>
<td>The dialing prefix assigned to the MCU, if any. MCUs without a prefix are unavailable for direct prefix-based dialing. MCUs do not need a prefix to be used as conferencing resources by the Conference Manager. Gateways do not need a direct dial-in prefix if you define simplified ISDN gateway dialing prefixes so that the RealPresence DMA system can choose from a pool of available gateways.</td>
</tr>
<tr>
<td>Strip prefix</td>
<td>When checked, the system strips the prefix when a call that includes a prefix is routed to this MCU.</td>
</tr>
</tbody>
</table>

### Bandwidth and Registration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class of service</td>
<td>When checked, you can specify the default class of service and the bit rate limits for this MCU. If specified, calls to this MCU use its class of service or the calling endpoint's, whichever is better.</td>
</tr>
<tr>
<td>Maximum bit rate (kbps)</td>
<td>Select the maximum bit rate for calls to this MCU.</td>
</tr>
<tr>
<td>Minimum downspeed bit rate (kbps)</td>
<td>Select the minimum bit rate to which calls to this MCU can be downspeeded to manage bandwidth. If this minimum is not available, the call is dropped. The minimum that applies to a call is the higher of the MCU's and the calling endpoint's.</td>
</tr>
<tr>
<td>Permanent</td>
<td>Prevents the MCU's registration with the Call Server from ever expiring. This option should always be selected.</td>
</tr>
<tr>
<td>Alert when MCU unregisters</td>
<td>If the MCU unregisters from the Call Server or its registration expires (if the <strong>Permanent</strong> check box is not selected), an informational alert is triggered.</td>
</tr>
</tbody>
</table>
### ISDN Gateway Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enable ISDN GW Function | When checked, makes the MCU available for selection as an ISDN gateway device and enables configuration of gateway session profiles. Gateway session profiles indicate to the MCU the bandwidth parameters to be used for the ISDN connection. Session profiles can be used for:  
  - ISDN gateway calls to the MCU’s direct dial-in prefix. In this case, the caller specifies the session profile prefix in the dial string:  
    `<direct dial-in prefix><session profile prefix><delimiter><E.164 number>`  
  - Calls to simplified ISDN gateway dialing prefixes. In this case, the RealPresence DMA system selects the MCU/gateway and its session profile. |
| Copy from entry for ISDN gateway | Enables copying the delimiter and session profiles from another ISDN gateway instead of entering them. Useful for MGC devices because each ISDN network card must be registered separately, but all cards support the same gateway configuration. |
| Dial string delimiter | The dial string delimiter used to separate the session profile prefix from the ISDN E.164 number. |
| Session Profile table | Lists the defined session profile prefixes. A session profile prefix is a numeric dial string prefix that specifies a bit rate for the call and the protocols it supports. Click Add to add a session profile. Click Edit or Delete to change or delete the selected profile. You cannot change or delete session profiles that the MCU/gateway used to register, but you can change or delete session profiles that you added. |
| Postliminary | A postliminary is an executable script, written in the Javascript language, that defines dial transformations to be applied before routing the call to the MCU/gateway. |
| Enabled | Lets you turn a postliminary on or off without deleting it. |
| Script | Type (or paste) the postliminary script you want to apply. Then click Debug this Script to open Test Preliminary and Postliminary Scripts and test the script with various variables. |

4 To reserve some of the MCU’s capacity for non-DMA use, set **Video ports reserved for non-DMA use** and **Voice ports reserved for non-DMA use** to the desired values.

5 To use a gateway-capable MCU as an ISDN gateway, go to **ISDN Gateway Settings** and complete the following steps:
   a Select the **Enable ISDN GW Function** check box.
   b Specify a **Dial string delimiter** and add one or more session profiles.

6 Click **OK**.

   The new MCU appears in the MCUs list. If the MCU is configured as a conferencing resource, it is placed into service.

7 If the MCU is configured as a conferencing resource, add it to the desired MCU pool(s).
Edit an MCU

You can edit the settings of an MCU.

If you need to edit the login information for the MCU (Management IP, Admin ID, or Password), you must first stop using the MCU (terminating existing calls and conferences) or busy it out and wait for existing calls and conferences to end.

Ensure that an MCU is not in use before editing its settings.

To edit an MCU:

1. On the Dashboard, verify that there are no calls and conferences on the MCU you want to edit.
2. Go to Integrations > MCU.
3. In the Actions list, click Edit.
4. In the Edit MCU dialog, edit the fields in the following table as required.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>External MCU</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Name for the MCU (up to 32 characters; must not include any of the following: , ; ; ? ; = *).</td>
</tr>
<tr>
<td>Type</td>
<td>Lists the types of MCUs the system supports. Must be set to the correct MCU type in order for the RealPresence DMA system to be able to connect to it. For an MGC MCU, this must be set to Polycom MGC gateway, even if it's being used as a standalone MCU.</td>
</tr>
<tr>
<td>Management IP address</td>
<td>Host name or IP address for logging into the MCU (to use it as a conferencing resource). <strong>Note:</strong> Polycom MCUs do not include their management IP address in the Subject Alternate Name (SAN) field of the CSR (Certificate Signing Request), so their certificates identify them only by the Common Name (CN). Therefore, if Skip validation of certificates received while making outbound connections is off in Security Settings, the MCU's management interface must be identified by the name specified in the CN field (usually the FQDN), not by IP address.</td>
</tr>
<tr>
<td>Admin user ID</td>
<td>Administrative user ID with which the Polycom RealPresence DMA system can log into the MCU.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the administrative user ID.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Video ports reserved for non-DMA use      | The number of video ports on this MCU that are off-limits to the Polycom RealPresence DMA system.  
**Note**: This feature is not for use with an integrated Polycom RealPresence Resource Manager system. The RealPresence Resource Manager system must have exclusive use of any MCUs on which it directly schedules conferences. When adding an MCU for use by a RealPresence Resource Manager system, the option **Enable for conference rooms** should not be selected in the settings dialog for that MCU. A Polycom MCU can be managed by the RealPresence Resource Manager system or the RealPresence DMA system, not both. |
| Voice ports reserved for non-DMA use       | The number of voice ports on this MCU that are off-limits to the Polycom RealPresence DMA system.  
**Note**: This feature is not for use with an integrated Polycom RealPresence Resource Manager system. The RealPresence Resource Manager system must have exclusive use of any MCUs on which it directly schedules conferences. When adding an MCU for use by a RealPresence Resource Manager system, the option **Enable for conference rooms** should not be selected in the settings dialog for that MCU. A Polycom MCU can be managed by the RealPresence Resource Manager system or the RealPresence DMA system, not both. |
| Cascade-for-size reserved video ports      | The number of video ports on this MCU to reserve for cascade links when a conference that has cascade for size enabled is created on this MCU.                                                                                                                                                                                                                  |
|                                           | **Per-conference**  
For each cascade-for-size conference on this MCU, this number of video ports is subtracted from the number of video ports available for participants. These ports are instead reserved for cascade links.                                                                                                                                                                              |
|                                           | **Overall**  
The number of video ports reserved for cascade-for-size cascade links on this MCU (in addition to the **Per-conference** value).                                                                                                                                                                                                                         |
| Strip prefix                               | If selected, the system strips the prefix when a call that includes a prefix is routed to this MCU.                                                                                                                                                                                                                                                                 |
| Direct dial-in prefix                      | The dialing prefix assigned to the MCU, if any. MCUs without a prefix are unavailable for direct prefix-based dialing.  
MCUs do not need a prefix to be used as conferencing resources by the Conference Manager.  
Gateways do not need a direct dial-in prefix if you define simplified ISDN gateway dialing prefixes so that the RealPresence DMA system can choose from a pool of available gateways.                                                                                           |
| Signaling IP for H.323                     | The dialing prefix assigned to the MCU, if any. MCUs without a prefix are unavailable for direct prefix-based dialing.  
MCUs don’t need a prefix to be used as conferencing resources by the Conference Manager.  
Gateways don’t need a direct dial-in prefix if you define simplified ISDN gateway dialing prefixes so that the RealPresence DMA system can choose from a pool of available gateways.                                                                                           |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signaling IP for SIP</td>
<td>The address that the MCU uses for SIP signaling. If you specify the login information for the MCU, this field is optional (the system can get the address from the MCU). If not, and SIP is enabled, this field is required.</td>
</tr>
<tr>
<td>Transport type</td>
<td>The SIP transport type to use with this MCU. If the Polycom RealPresence DMA system’s security settings don’t allow unencrypted connections, this must be TLS.</td>
</tr>
<tr>
<td>Signaling type</td>
<td>Select SIP, H.323, or both, depending on the configuration of the Polycom RealPresence DMA system and the MCU.</td>
</tr>
<tr>
<td>Enable for conference rooms</td>
<td>Makes the MCU available as a conferencing resource for the Polycom RealPresence DMA system's Conference Manager. Up to 64 MCUs can be enabled for conference rooms. <strong>Caution:</strong> Before adding an MCU to the RealPresence DMA system’s conferencing resources, make sure that MCU isn’t already a RealPresence Resource Manager system conferencing resource. The RealPresence Resource Manager system must have exclusive use of any MCUs on which it directly schedules conferences.</td>
</tr>
</tbody>
</table>
| Enable gateway profiles   | Makes the MCU available for selection as an ISDN gateway device and enables the Gateway Profiles tab for configuring gateway session profiles. Gateway session profiles indicate to the MCU the bandwidth parameters to be used for the ISDN connection. They can be used for:  
  • ISDN gateway calls to the MCU’s direct dial-in prefix. In this case, the caller specifies the session profile prefix in the dial string:  
    `<direct dial-in prefix><session profile prefix><delimiter><E.164 number>`  
  • Calls to simplified ISDN gateway dialing prefixes. In this case, the RealPresence DMA system selects the MCU/gateway and its session profile.                                                                                                                                                        |
| Class of service          | Select to specify the default class of service and the bit rate limits for this MCU. If specified, calls to the MCU use its class of service or the calling endpoint’s, whichever is better.                                                                                                                                                                                                 |
| Maximum bit rate (kbps)   | Select the maximum bit rate for calls to this MCU.                                                                                                                                                                                                                                                                                                 |
| Minimum downspeed bit rate (kbps) | Select the minimum bit rate to which calls to this MCU can be downspeeded to manage bandwidth. If this minimum isn’t available, the call is dropped. The minimum that applies to a call is the higher of the MCU’s and the calling endpoint’s.                                                                                                           |
| Permanent                 | Prevents the MCU’s registration with the Call Server from ever expiring. For MCUs, this option should always be selected (the default).                                                                                                                                                                                                                   |
| Alert when MCU unregisters | If the MCU unregisters from the Call Server or its registration expires (if Permanent is turned off), an informational alert is triggered (see Alert 5003).                                                                                                                                                                                                 |
To set aside more or fewer ports for non-DMA use, change the **Video ports reserved for non-DMA use** and **Voice ports reserved for non-DMA use** values.

Note: This feature is not for use with a Polycom RealPresence Resource Manager system. The RealPresence Resource Manager system must have exclusive use of any MCUs on which it directly schedules conferences (direct conferences). When adding an MCU for use by a RealPresence Resource Manager system, the option **Enable for conference rooms** should not be selected in the settings dialog for that MCU.

To use a gateway-capable MCU as an ISDN gateway, select the **Enable gateway profiles** check box and, on the **Gateway Profiles** tab, specify a dial string delimiter and add or change session profiles. To stop using it, clear the **Enable gateway profiles** check box.

Click **OK**.

If the MCU is configured as a conferencing resource, optionally change the MCU pool(s) to which it's assigned.

Pools and pool orders are used to determine which MCU is used for a conference.

---

### Gateway Profiles

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy from entry for ISDN gateway</td>
<td>Lets you copy the delimiter and session profiles from another ISDN gateway. This is especially useful for MGC devices because each ISDN network card must be registered separately, but all cards support the same gateway configuration.</td>
</tr>
<tr>
<td>Dial string delimiter</td>
<td>The dial string delimiter used to separate the session profile prefix from the ISDN E.164 number.</td>
</tr>
<tr>
<td>Session Profile table</td>
<td>Lists the defined session profile prefixes. A session profile prefix is a numeric dial string prefix that specifies a bit rate for the call and which protocols it supports. Click <strong>Add</strong> to add a session profile. Click <strong>Edit</strong> or <strong>Delete</strong> to change or delete the selected profile. You can’t change or delete session profiles that the MCU/gateway registered with, only those that you added.</td>
</tr>
</tbody>
</table>

### Media IP Addresses

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add new media IP address</td>
<td>If you specify the login information for the MCU, the system can get media addresses from the MCU. If not, enter an IP address for media streams and click <strong>Add</strong> to add it to the list below.</td>
</tr>
<tr>
<td>Media IP addresses</td>
<td>List of media addresses for the MCU. Click <strong>Remove</strong> to delete the selected address.</td>
</tr>
</tbody>
</table>

### Postliminary

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Lets you turn a postliminary on or off without deleting it.</td>
</tr>
<tr>
<td>Script</td>
<td>Type (or paste) the postliminary script you want to apply. Then click <strong>Debug this Script</strong> to open <strong>Test Preliminary and Postliminary Scripts</strong> and test the script with various variables.</td>
</tr>
</tbody>
</table>

---

5 To set aside more or fewer ports for non-DMA use, change the **Video ports reserved for non-DMA use** and **Voice ports reserved for non-DMA use** values.

6 To use a gateway-capable MCU as an ISDN gateway, select the **Enable gateway profiles** check box and, on the **Gateway Profiles** tab, specify a dial string delimiter and add or change session profiles. To stop using it, clear the **Enable gateway profiles** check box.

7 Click **OK**.

8 If the MCU is configured as a conferencing resource, optionally change the MCU pool(s) to which it’s assigned.

Pools and pool orders are used to determine which MCU is used for a conference.
Add a Session Profile

You can add a session profile to the ISDN gateway if the selected MCU is enabled as an ISDN gateway device.

To add a session profile:
1. Go to Integrations > MCUs and do one of the following:
2. Select an existing MCU and click Edit.
3. Select ISDN Gateway Settings.
4. Select Enable ISDN GW Function.
5. Click Add.
6. Fill in the fields in the following table as required.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session profile prefix</td>
<td>Numeric dial string prefix for this profile.</td>
</tr>
<tr>
<td>Bit rate</td>
<td>Bit rate of calls using this profile.</td>
</tr>
<tr>
<td>H.320</td>
<td>Select the protocol(s) for this profile.</td>
</tr>
<tr>
<td>H.323</td>
<td>Only H.320 and PSTN are relevant when adding a profile. The others are</td>
</tr>
<tr>
<td>PSTN</td>
<td>selected if the gateway specified them when registering.</td>
</tr>
<tr>
<td>SIP</td>
<td></td>
</tr>
</tbody>
</table>

7. Click OK.
   The new session profile appears in the list.

Edit a Session Profile

You can edit a session profile that you added. You cannot edit session profiles with which the MCU/gateway registered.

To edit a session profile:
1. On the Integrations > MCU page, select an MCU and click Edit to open the Edit MCU dialog.
2. Select the Gateway Profiles tab in the Edit MCU dialog.
3. Select a session profile from the list.
4. Click Edit.
5. Fill in the fields in the following table as required.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session profile prefix</td>
<td>Numeric dial string prefix for this profile.</td>
</tr>
</tbody>
</table>
Delete an MCU

You can delete an MCU to remove it as an available conferencing resource. You cannot delete an MCU if either of the following conditions is true:

- The MCU is hosting one or more conferences. You can delete the MCU after you busy it out and wait for all conferences to end.
- The MCU is registered with the Call Server. You can delete the MCU after you unregister it.

To delete an MCU:

1. On the Dashboard, verify that there are no calls and conferences on the MCU you want to delete.
2. Go to Integrations > MCUs.
3. In the MCUs list, select the MCU to delete.
4. In the Actions list, click Delete.
5. Click Yes to confirm.

Stop Using an MCU

You can immediately stop the RealPresence DMA system from using one or more MCUs as conferencing resources or ISDN gateways. This action terminates all conference activity on the MCU.

The RealPresence DMA system immediately terminates all H.323 calls and conferences that it placed on the MCUs you stop using. For SIP calls, the system migrates the calls to in-service MCUs that have available capacity. The RealPresence DMA system will not select MCUs you have stopped using for any future conferences and simplified ISDN dialing calls.

Note that this command terminates the RealPresence DMA system's use of an MCU, but the MCU can continue to accept any calls from other sources.

To stop using an MCU:

1. Go to Integrations > MCUs.
2. In the MCUs list, select the MCU to stop using.
3. In the Actions list, click Stop Using.
4 Click Yes to confirm.

Start Using an MCU Again

You can put an MCU back in service again for conferencing and simplified gateway dialing if it has been stopped or busied out.

This command only affects Conference Manager and simplified gateway dialing functionality; it does not affect MCUs that are simply registered with the Call Server.

To start an MCU again:
1 Go to Integrations > MCUs.
2 In the MCUs list, select the stopped or busied-out MCU to start using again.
3 In the Actions list, click Start Using.

Busy Out an MCU

The Polycom RealPresence DMA system stops creating new conferences on MCUs that you busy out, but it allows existing conferences to continue and accepts new calls to those conferences. The system also excludes busied-out MCUs from consideration for simplified ISDN dialing calls.

To busy out an MCU:
1 Go to Integrations > MCUs.
2 In the MCUs list, select one or more MCUs to busy out.
3 In the Actions list, click Busy Out.
4 Click Yes to confirm.

Quarantine an MCU

A quarantined MCU is able to register (or remain registered) with the Call Server, but is not able to make or receive calls.

Quarantining is intended only for MCUs that are registered with the Polycom RealPresence DMA system's Call Server as standalone MCUs and/or ISDN gateways, but are not available to the Conference Manager as conferencing resources.

To quarantine an MCU:
1 Go to Integrations > MCUs.
2 In the MCUs list, select the MCU to quarantine.
3 In the Actions list, click Quarantine.
Unquarantine an MCU

If you quarantine one or more MCUs, the **Unquarantine** option becomes available in the **Actions** list. When you unquarantine an MCU that is registered with the Call Server, it is able to make or receive calls again.

**To unquarantine an MCU:**
1. Go to **Integrations > MCUs**.
2. In the MCUs list, select the MCU to unquarantine.
3. In the **Actions** list, click **Unquarantine**.

Block Registrations From an MCU

You can prevent one or more MCUs from registering with the Call Server.

**To block registrations from an MCU:**
1. Go to **Integrations > MCUs**.
2. In the MCUs list, select the MCU to prevent from registering with the Call Server.
3. In the **Actions** list, click **Block Registrations**.

Unblock Registrations From an MCU

If one or more MCUs are blocked, the **Unblock Registrations** option becomes available in the **Actions** list. You can allow one or more MCUs to register with the Call Server by unblocking them.

**To unblock registrations from an MCU:**
1. Go to **Integrations > MCUs**.
2. In the MCUs list, select the MCU to unblock from registering with the Call Server.
3. In the **Actions** list, click **Unblock Registrations**.

View Call History

You can view the call history report for an MCU.

**To view call history:**
1. Go to **Integrations > MCUs**.
2. In the MCUs list, select the MCU with the call history you want to view.
3. In the **Actions** list, click **View Call History**. The call history report displays.
MCU Pools and Pool Orders

The RealPresence DMA system requires you to create uses MCU pools, or logical groupings of media servers, before you can use an MCU as a conferencing resource. You can determine how to group MCU pools. For example, you can base an MCU pool on location, capability, or some other factor.

After creating the MCU pools you need, you can configure a Pool Order. A pool order contains one or more MCU pools and specifies the order of preference in which the RealPresence DMA system will use the pools. The RealPresence DMA system uses the pool(s) to which an MCU belongs, and the pool order(s) to which a pool belongs, to determine which MCU will host a conference.

Every conference room (VMR) is associated with an MCU pool order by direct assignment, through the user’s enterprise group membership, or from the system default).

Note: MCU pools and pool orders are not used to select an ISDN gateway for simplified gateway dialing.

You can use various criteria for organizing MCUs into pools, depending on how you want the MCU resources allocated for conferencing. For instance:

- Assign all MCUs in a specific site or domain to a pool. Then, assign a pool order to all users in that site or domain (via group membership), ensuring that their conferences are preferentially routed to MCUs in that pool.
- Assign one or more MCUs to a pool to be used only by executives and assign that pool to a pool order associated only with those executives’ conference rooms.
- Assign MCUs with special capabilities to a pool and assign that pool to a pool order associated only with custom conference rooms requiring those capabilities.

MCU Selection Process

The Polycom RealPresence DMA system can assess only the resources that an MCU currently has available. The system cannot assess the resources that have been scheduled for future use.

The RealPresence DMA system chooses an MCU for a user’s conference by applying the following rules in order:

1. Select the MCU pool order:
   a. Use the pool order directly assigned to the user’s conference room.
   b. If none, use the highest priority pool order associated with any group to which the user belongs.
   c. If none, use the system default.
2. Select the first MCU pool in the MCU pool order.
3 Select the best MCU in the MCU pool, based on how well their capabilities fulfill the user’s needs in the following respects:

- MCU has RealPresence Collaboration Server or RMX profile required by user’s conference template.
- MCU has IVR service required by user’s conference template.
- MCU has recording capability required by user’s conference template.
- MCU supports WebRTC clients.
- MCU supports SVC conferencing.
- MCU supports cascaded conferences with both on-premises and external Skype for Business AVMCs.

If there are multiple MCUs that are equally capable, select the least used, as determined by the following formula:

\[
\text{port\_availability} = \left( \frac{\text{free\_video\_ports}}{\text{total\_video\_ports}} \right) + (0.0001 \times \frac{\text{free\_audio\_ports}}{\text{total\_audio\_ports}})
\]

\[
\text{mixer\_availability} = \left( \frac{\text{total\_video\_ports} - 2 \times \text{active\_dma\_conferences}}{\text{total\_video\_ports}} \right) + 0.0001 \times \left( \frac{\text{total\_audio\_ports} - 2 \times \text{active\_dma\_conferences}}{\text{total\_audio\_ports}} \right)
\]

\[
\text{availability} = \min (\text{port\_availability}, \text{mixer\_availability})
\]

4 If no MCUs in the selected MCU pool have capacity, select the next MCU pool in the pool order and return to step 3.

5 If no MCUs are available in any of the MCU pools in the pool order:

- If fallback is enabled, select the best MCU available to the Polycom RealPresence DMA system, based on the system’s capability algorithm.
- If fallback is not enabled, reject the call.

On the Service Config > Conference Manager Settings > Conference Settings page, when the MCU Selection field is set to Prefer MCU in first caller’s site, the system will match the MCU chosen for the call with the site that the first caller’s endpoint belongs to.

On the Service Config > Conference Manager Settings > Conference Templates page, under the Add/Edit Conference template > RMX General Settings dialog, the Cascade for Size option enables conferences using this template to span Polycom MCUs to achieve conference sizes larger than a single MCU can accommodate.

If Cascade for Size is enabled and the MCU Selection field is set to Prefer MCU in first caller’s site, the rules for Cascade for size take precedence over the rules for Prefer MCU in first caller’s site during MCU selection. This is because if a conference starts on an MCU with insufficient ports reserved for Cascade for size, then that conference will never cascade.

### MCU Availability and Reliability Tracking

In order to minimize the number of failed calls, the Polycom RealPresence DMA system employs mechanisms for detecting and handling MCU availability and reliability issues:

- If it can’t reach an MCU’s management interface, the RealPresence DMA system won’t route calls to that MCU.
- If an MCU reports zero capacity via its management interface, the RealPresence DMA system won’t route calls to that MCU.
When calls to a specific MCU fail, the RealPresence DMA system reduces the MCU’s reliability score, causing it to be selected less frequently than other MCUs.

An MCU’s reliability depends on the number of consecutive failed calls. As that number increases, the RealPresence DMA system treats a growing percentage of the MCU’s ports as if they were in use. Since the RealPresence DMA system selects the least used of the capable MCUs in its pool, the likelihood that an MCU with failures will be chosen for the next call declines rapidly (depending on the number of consecutive failed calls and the remaining capacity in the MCU pool).

Every 30 minutes, the reliability score of the MCU is increased so that it won’t be permanently removed from the pool due to failures in the past. To avoid trying the MCU every 30 minutes, monitor the RealPresence DMA system and administratively take the MCU out of service.

By increasing the number of MCUs in the pool or increasing their capacity, you can decrease the usage of the working MCUs during a failover scenario. So, for example, if you want to avoid routing any more calls to an MCU after two consecutive failed calls, provide enough excess capacity that the remaining MCUs never all reach 43% port usage during a failure.

### Working with MCU Pools

After you manually add an MCU to your Polycom® RealPresence® DMA® system, you need to add it to an MCU pool so it can be used as a conference resource. Conferencing resources can be assigned for use in conferences. Note that MCUs that are registered to the RealPresence DMA system (not added by you), cannot be added to an MCU pool.

### View MCU Pools

You can view a list of MCU pools you have created.

To view MCU pools:

» Go to Service Config > Conference Manager Settings > MCU Pools.

The following table describes the fields in the list.
Add an MCU Pool
You can define a new MCU pool in the RealPresence DMA system.

To add an MCU pool:
1. Go to Service Config > Conference Manager Settings > MCU Pools.
2. In the Actions list, click Add.
3. In the Add MCU Pool dialog, enter a name and description for the MCU pool.
4. In the Edit MCU Pool dialog, change the name or description for the MCU pool if desired.
5. Select the MCUs you want to include in the pool by using the arrow buttons to move MCUs from the Available MCUs list to the Selected MCUs list.
6. Click OK.

   The new MCU pool appears in the MCU Pools list. The MCUs included in the pool are displayed.

Edit an MCU Pool
You can edit an existing MCU pool at any time.

To edit an MCU pool:
1. Go to Service Config > Conference Manager Settings > MCU Pools.
2. In the MCU Pools list, select the pool, and in the Actions list, click Edit.
3. In the Edit MCU Pool dialog, change the name or description for the MCU pool if desired.
4. Select the MCUs you want to include in the pool by using the arrow buttons to move MCUs from the Available MCUs list to the Selected MCUs list.
5. Click OK.

   The changes you made appear in the MCU Pools list.

Delete an MCU Pool
You can delete an MCU pool if it is no longer needed.

To delete an MCU Pool:
1. Go to Service Config > Conference Manager Settings > MCU Pools.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the MCU pool.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the pool, such as the geographic location of the MCUs it contains.</td>
</tr>
<tr>
<td>MCUs</td>
<td>The MCUs that are in the pool.</td>
</tr>
</tbody>
</table>
2 In the **MCU Pools** list, select the MCU pool you want to remove.

3 In the **Actions** list, select **Delete**.

   If the pool is included in one or more pool orders, the system warns you and provides information about the consequences of deleting it.

4 When asked to confirm that you want to delete the selected MCU pool, click **Yes**.

### Working with MCU Pool Orders

A pool order contains one or more MCU pools and specifies the order of preference in which the pools are used. Every conference room (VMR) is associated with an MCU pool order in one of the following ways:

- By direct assignment.
- Via the user’s enterprise group membership.
- From the system default.

The pool(s) to which an MCU belongs, and the pool order(s) to which a pool belongs, are used to determine which MCU is used to host a conference.

You can configure an MCU pool order to fall back to *any* available MCU if no MCU within the pool order’s selected pools is available to host a conference. When the system selects an MCU based on the "Fall back to any available MCU" setting, the selected MCU is considered to be a member of the pool order.

MCU pools and pool orders are not used to select an ISDN gateway for simplified gateway dialing.

### Naming Conventions for Pool Orders

If you have a Polycom RealPresence Resource Manager system that is configured to schedule conferences on the RealPresence DMA system’s conferencing resources (MCU pools), you must create MCU pools and pool orders specifically for use by the RealPresence Resource Manager system. The pool orders should be named in such a way that:

- They appear at the top of the pool order list presented in the RealPresence Resource Manager system.
- Users will understand that they should choose one of the RealPresence Resource Manager system's pool orders.

### View MCU Pool Orders

You can view MCU pool orders. In a superclustered system, this list is the same on all clusters in the supercluster.
To view MCU pool orders:

» Go to Service Config > Conference Manager Settings > MCU Pool Orders.

The following table describes the fields in the list.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Priority ranking of the pool order.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the pool order.</td>
</tr>
<tr>
<td>Description</td>
<td>Brief description of the pool order.</td>
</tr>
<tr>
<td>MCU Pools</td>
<td>The MCU pools that are in the pool order.</td>
</tr>
<tr>
<td>Fallback</td>
<td>Indicates whether this pool order is configured to use any available MCU if none are available in its pools.</td>
</tr>
</tbody>
</table>

**Add an MCU Pool Order**

You can add an MCU pool order to specify the order of preference in which the RealPresence DMA system uses existing MCU pools.

To add an MCU pool order:

1. Go to Service Config > Conference Manager Settings > MCU Pool Orders.
2. In the Actions list, click Add.
3. In the Add MCU Pool Order window, complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the MCU pool order.</td>
</tr>
<tr>
<td>Description</td>
<td>Brief description of the pool order.</td>
</tr>
<tr>
<td>Available MCU pools</td>
<td>Lists the MCU pools available to the system.</td>
</tr>
<tr>
<td>Selected MCU pools</td>
<td>Lists the pools included in the pool order in their priority order. The left/right arrow buttons move pools in and out of the list. The up/down arrow buttons change the priority rankings of the pools.</td>
</tr>
<tr>
<td>Fall back to any available MCU</td>
<td>Indicates whether this pool order will use any available MCU if there are no available MCUs in this pool order’s pools.</td>
</tr>
</tbody>
</table>

4. Click OK.

The new MCU pool order appears in the MCU Pool Orders list. The MCU pools included in the pool order are displayed.

**Edit an MCU Pool Order**

Once you create an MCU pool order, you can change it at any time.
To edit an MCU pool order:

1. Go to Service Config > Conference Manager Settings > MCU Pool Orders.
2. In the MCU Pool Orders list, select the pool order, and in the Actions list, click Edit.
3. In the Edit MCU Pool Order dialog, edit the following fields as required.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the MCU pool order.</td>
</tr>
<tr>
<td>Description</td>
<td>Brief description of the pool order.</td>
</tr>
<tr>
<td>Available MCU pools</td>
<td>Lists the MCU pools available to the Polycom RealPresence DMA system.</td>
</tr>
<tr>
<td>Selected MCU pools</td>
<td>Lists the pools included in the pool order in their priority order. The left/right arrow buttons move pools from one list to the other. The up/down arrow buttons change the priority rank of the selected pool.</td>
</tr>
<tr>
<td>Fall back to any available MCU</td>
<td>Indicates whether this pool order is set to fall back to any available MCU if there are no available MCUs in its pools.</td>
</tr>
</tbody>
</table>

4. Click OK.
   
The changes you made appear in the MCU Pool Orders list.

**Edit the Priority Ranking of a Pool Order**

You can modify the priority in which a pool order is used.

To modify the priority of a pool order:

1. Go to Service Config > Conference Manager Settings > MCU Pool Orders.
2. Select the MCU you want to change.
3. In the Actions list, click Move Up or Move Down until the MCU is in the desired position in the list.

**Delete an MCU Pool Order**

If an MCU pool order is no longer needed, you can delete it from the system.

To delete an MCU pool order:

1. Go to Service Config > Conference Manager Settings > MCU Pool Orders.
2. In the MCU Pool Orders list, select the pool order, and in the Actions list, select Delete.
3. When asked to confirm that you want to delete the selected MCU, click Yes.
Integration with Other Services

This section provides an introduction to integrating the Polycom® RealPresence® DMA® system with other services on your network. It includes:

- Microsoft® Active Directory® Integration
- Microsoft® Skype® for Business Integration
- Microsoft Exchange Server Integration
- RealPresence Resource Manager Integration
Microsoft® Active Directory® Integration

When you integrate the Polycom® RealPresence® DMA system® with your Microsoft® Active Directory®, the enterprise users (Active Directory members) become Conferencing Users in the Polycom RealPresence DMA system. Each enterprise user is (optionally) assigned a conference room or Virtual Meeting Room (VMR). The conference room IDs are typically generated from the enterprise users' phone numbers.

Once integrated with Active Directory, the Polycom RealPresence DMA system accesses the directory under the following circumstances:

- Nightly, to update the user and group information in its cache.
- Whenever you force a cache refresh using the Update button.
- To authenticate login passwords.
- To create or delete Polycom conference contacts whenever a publishable VMR is created or deleted (only if the RealPresence DMA system is integrated with Microsoft Lync 2013 or Skype for Business and contact creation is enabled).

In a super-clustered environment, one cluster is responsible for integrating with Active Directory and updating the cache daily, and the cache is available to all clusters through the replicated shared data store. The other clusters connect to Active Directory only to authenticate user credentials.

Integrate with Active Directory

You can enable integration with Active Directory. Before integrating, read Set Up Security and Connect to Microsoft Active Directory®. You should also know approximately how many enterprise users you expect the system to retrieve.

If you have a Polycom RealPresence Resource Manager system, be aware that the machine account used for AD integration by the RealPresence Resource Manager system and the service account used for AD integration by the RealPresence DMA system have different requirements. Do not try to use the same account for both purposes.

If you use Active Directory attributes that are not replicated across the enterprise through the Global Catalog server mechanism, the system must query each domain for the data. Make sure that the whitelist for the service account that the RealPresence DMA system uses is correct and that it can connect to all the LDAP servers in each domain.

Unless the Allow unencrypted connections to the Active Directory security option is enabled, the RealPresence DMA system offers the same SSL server certificate that it offers to browsers connecting to the system’s management interface. The Microsoft Active Directory server must be configured to trust the certificate authority.
To integrate with Active Directory:

1. In Windows Server, add the service account (read-only user account) that the RealPresence DMA system will use to read the Active Directory and configure the account as follows:
   - User can not change password.
   - Password never expires.
   - User can only access services on the domain controllers and cannot log in anywhere.
   If you are integrating the RealPresence DMA system with Lync 2013 or Skype for Business and plan to use the automatic conference contact creation feature, the service account you create here should have full permissions to add, change, and delete entries in the OU where the conference contacts are stored, along with full administrative permissions for Lync or Skype administration to manipulate these contacts.

2. In the RealPresence DMA system, replace the default local administrative user with your own user account that has the same user roles.

3. Log in to the RealPresence DMA system as the local user you created in the preceding step and go to Integrations > Microsoft Active Directory.

4. Check Integrate with Enterprise Directory Server and complete the information in the General Integration Settings section.
   a. Do one of the following:
      - Unless you have a single domain environment and no global catalog, select Auto-discover and enter the DNS domain name.
      - Select IP Address or FQDN and enter the appropriate value.
   b. For Domain\Enterprise Directory User ID, enter the domain and user ID of the account that you created previously.
   c. For Enterprise Directory User Password, enter the password of the account you created previously.
   d. Leave Security Level set to the default Automatic.
   e. Edit the User LDAP filter expression only if you understand LDAP filter syntax (see RFC 2254) and know what changes to make.
   f. Leave Base DN set to the default All Domains.

5. Complete the information in the Cache Refresh section.
   a. Specify how many times per day the RealPresence DMA should check the Active Directory for changes.
      Consider the information in Active Directory Cache Refresh Frequency when configuring cache refresh settings.
   b. Specify the time of day the RealPresence DMA system should check the Active Directory for changes.
   c. Select the territory whose cluster should perform the integration and daily updates.
6 To generate conference room IDs for the enterprise users, complete the Enterprise Conference Room ID Generation section.
Skip this step if you do not want the system to create conference rooms (virtual meeting rooms) for the enterprise users.

- **a** Specify the Active Directory attribute from which to generate unique room IDs, typically phone numbers or employee ID numbers.
- **b** If necessary, edit the contents of the Characters to remove field.
  - If you use phone numbers, the default contents of this field should be adequate to ensure a numeric room ID.
- **c** Specify the number of characters to use.
  - After the system strips out characters to remove, it removes characters in excess of this number from the beginning of the string.

7 If your environment uses external Lync or Skype for Business systems, enable the Callback contacts OU field and enter the path of a container that contains callback contact accounts for use with external Skype systems.

For information on how to configure callback contact accounts in Active Directory, see the Polycom Unified Communications for Microsoft Environments - Solution Deployment Guide.

8 Click Update.
After a short time, the system confirms that Active Directory configuration has been updated.

9 Note the time and click OK.

10 To restrict the RealPresence DMA system to work with a subset of the Active Directory (such as one tree of multiple trees, a subtree, or a domain), repeat steps 4 to step 8, selecting the value you want from those now available in the Base DN list. See Understanding Base DN.

11 Check the Total users/rooms and Conference room errors values. If the numbers are significantly different from what you expected, you'll need to investigate after you complete the next step (you must be logged in as an enterprise user to investigate further).

12 Set up your enterprise account and secure the service account:
- **a** Log out and log back in using the service account you created in step 1.
  - You must be logged in with an Active Directory user account to see other enterprise users. Use the service account user ID created in the initial step.
- **b** Go to User > Users, clear the Local users only check box, locate your named enterprise account, and give it Administrator privileges.
- **c** Log out and log back in using your named enterprise account.
- **d** Secure the service account by removing all user roles and marking it disabled in the RealPresence DMA system (not in the Active Directory) so that this account cannot be used for conferencing or for logging in to the Polycom RealPresence DMA system management interface.

13 If the Total users/rooms values were significantly different from what you expected, try to determine the reason and fix it:
a Go to **User > Users** and perform some searches to determine which enterprise users are available and which aren’t.

b If there are many missing or incorrect users, consider whether changes to the LDAP filter can correct the problem or if there is an issue with the directory integration configuration chosen.

14 If there were many conference room errors, try to determine the reason and fix it:

a Go to **Reports > Conference Room Errors** and verify that the time on the report is after the time when you received confirmation that the Active Directory is updated.

b Review the list of duplicate and invalid conference room IDs. Consider whether using a different Active Directory attribute, increasing the conference room ID length, or editing the characters to remove will resolve the majority of problems.

If there are only a few problems, they can generally be resolved by correcting invalid Active Directory entries.

15 If necessary, repeat steps 4 to step 11, steps 13, and 14, modifying the integration parameters as needed, until you get a satisfactory result.

### Understanding Base DN

The **Base DN** field is where you can specify the *distinguished name* (DN) of a subset of the Active Directory hierarchy (a domain, subset of domains, or organizational unit) to which you want to restrict the RealPresence DMA system. It acts like a filter.

The following diagram illustrates how choosing different Base DN values affects which parts of a forest are included in the directory integration.
The **Base DN** field defaults to *All Domains* (which is equivalent to specifying an empty base DN in a query). Initially, the only other option is to enter a custom DN value. The first time you tell the system to connect to the Active Directory server, leave **Base DN** set to *All Domains*.

After the system has successfully connected to the Active Directory, the list contains entries for each domain in the AD forest. If you want to restrict the system to a subset of the Active Directory (such as one tree of multiple trees, a subtree, a domain, or an organizational unit), select the corresponding base DN entry from the list.

### Adding Passcodes for Enterprise Users

You can add passcodes for enterprise users. Polycom MCUs provide two optional security features for conferences, which the Polycom RealPresence DMA system fully supports:
• Conference Passcode — A numeric passcode that callers must enter in order to join the conference.

• Chairperson Passcode — A numeric passcode that callers can enter to identify themselves as conference chairpersons. Chairpersons have additional privileges, such as controlling recording. A conference can be configured to not start until a chairperson joins and to end when the last chairperson leaves.

If Cisco Codian MCUs are included in the Polycom RealPresence DMA system’s pool of conferencing resources, do not assign a chairperson passcode without also assigning a conference passcode. If a conference with only one passcode (either chairperson or conference) lands on a Codian MCU, all callers to the conference must enter that passcode.

If the RealPresence DMA system is integrated with your Active Directory, conference and chairperson passcodes for enterprise users can be maintained in the Active Directory.

You must determine which Active Directory attributes to use for the purpose and provide a process for provisioning users with those passcodes. If a user’s passcode Active Directory attribute (either conference or chairperson) is left empty, the user’s conferences will not require that passcode.

Passcodes must consist of numeric characters only (the digits 0-9). You can specify the maximum length for each passcode type (up to 16 digits). A user’s conference and chairperson passcodes can not be the same.

When you generate passcodes for enterprise users, the RealPresence DMA system retrieves the values in the designated Active Directory attributes and removes any non-numeric characters from them. If the resulting numeric passcode is longer than the maximum for that passcode type, it strips the excess characters from the beginning of the string.

**Generate Chairperson and Conference Passcodes for Enterprise Users**

You can generate chairperson and conference passcodes for Enterprise users.

To generate chairperson and conference passcodes for enterprise users:

1 In the Active Directory, select an unused attribute to be used for each of the passcodes.

   In a multi-domain forest, it is best to choose attributes that are replicated across the enterprise via the Global Catalog server mechanism. But if the attributes you select are not available in the Global Catalog, the system can read them directly from each domain.

   You can use an existing attribute that contains numeric data, such as an employee ID. This may not provide much security, but might be sufficient for conference passcodes.

2 In the Active Directory, either provision users with passcodes or establish a mechanism for letting users create and maintain their own passcodes.

   Consult your Active Directory administrator for assistance with this.

3 On the Polycom RealPresence DMA system, go to **Integrations > Microsoft Active Directory**.

4 Complete the **Enterprise Chairperson and Conference Passcode Generation** section.
a Specify the Active Directory attribute from which to generate chairperson passcodes and the number of characters to use.

b Specify the Active Directory attribute from which to generate conference passcodes and the number of characters to use.

5 Click Update.

After a short time, the system confirms that Active Directory configuration has been updated.

6 Note the time. Click OK.

7 Confirm that passcode generation worked as expected.

a Go to Reports > Enterprise Passcode Errors and verify that the time on the report is after the time you got the confirmation that Active Directory configuration has be updated.

b Review the number of valid, invalid, and unassigned passcodes.

   If there are only a few problems, they can generally be resolved by correcting invalid Active Directory entries.

Duplicate and invalid passcodes should be avoided as they could indicate a problem with the type of data in the selected attributes or with the number of characters you elected to use.

Active Directory Cache Refresh Frequency

Periodically, the system must refresh its cache of users, groups, and conference rooms from Active Directory. As part of Active Directory integration, you can configure how often the system connects to Active Directory and updates its cache. Be aware that Active Directory cache refreshes can take a variable amount of time to complete, depending on the size of the directory and the amount of data being imported.

The initial import of data from Active Directory takes roughly three times as long as periodic refreshes. Active Directory cache refreshes may cause performance issues when the RealPresence DMA system is both under heavy call load and refreshing a large amount of data from the directory (many thousands of users). If a large number of users need to be imported from Active Directory and the RealPresence DMA system is subject to heavy call loads, you should schedule Active Directory cache refreshes during low-load hours.

Cache refresh times are scheduled for the timezone of the RealPresence DMA system where the refresh occurs, but are expressed in the timezone of the browser client. For example: You are located in New York and schedule a cache refresh for 6:00am on a RealPresence DMA system located in London. The cache refresh occurs at 6:00am in the London time zone, but the Active Directory Integration Dashboard pane shows the time of most recent refresh as 2:00am, which was the local time (in New York) when the refresh occurred (in London).

Orphaned Groups and Users

When you manually update your Active Directory connection or when the system updates the connection automatically to refresh it's cache, some Active Directory users and groups within the RealPresence DMA system may become "orphaned". Orphaned users and groups are no longer in the Active Directory or are no longer accessible to the Polycom RealPresence DMA system, but for which the system has local data (typically, local conference rooms or customized enterprise conference rooms).
Generate an Orphaned Groups and Users Report

You can generate an orphaned groups and users report.

To generate an orphaned users and groups report:

» Go to Reports > MS Active Directory Reports > Orphaned Groups and Users.

The following table describes the fields included in the report.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Orphaned Groups</td>
<td></td>
</tr>
<tr>
<td>Group ID</td>
<td>ID of the user group.</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain to which the user group belonged.</td>
</tr>
<tr>
<td>Orphaned Users</td>
<td></td>
</tr>
<tr>
<td>User ID</td>
<td>ID of the user.</td>
</tr>
<tr>
<td>First Name</td>
<td>The user’s first name.</td>
</tr>
<tr>
<td>Last Name</td>
<td>The user’s last name.</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain to which the user belonged.</td>
</tr>
<tr>
<td>Roles</td>
<td>Polycom RealPresence DMA system user roles assigned to the user.</td>
</tr>
<tr>
<td>Conference Rooms</td>
<td>Polycom RealPresence DMA system custom conference rooms assigned to the user.</td>
</tr>
</tbody>
</table>

Remove Orphaned Groups and Users

You can remove orphaned group data from the system.

Orphaned data is no longer usable by the system, so you can generally delete it. But first make sure that the system is successfully integrated to the correct active directory domain. Switching domains can cause many users and groups to be orphaned.

To remove orphaned group data from the system:

1. Go to Reports > MS Active Directory Reports > Orphaned Groups and Users.
2. In the Actions list, click Clean Orphaned Groups.
3. When prompted to confirm, click OK.

   The system removes the orphaned group data.
About the System’s Directory Queries

The Polycom RealPresence DMA system uses the following subtree scope LDAP queries. In a standard Active Directory configuration, all these queries use indexes.

- User Search
- Group Search
- Global Group Membership Search
- Attribute Replication Search
- Configurable Attribute Domain Search
- Domain Search
- Service Account Search

The system runs the first three queries every time it creates or updates its cache as follows:

- When you click Update on the Microsoft Active Directory page.
- When the system restarts (if integrated with Active Directory).
- At the scheduled daily cache refresh time.

User Search

The User Search queries the global catalog. In a standard AD configuration, all the filter attributes and attributes returned are replicated to the global catalog. The elements in italics are examples. The actual values of these variables depend on your configuration.

- Base: <empty>
  The base variable depends on the Base DN setting on the Microsoft Active Directory page. If it's set to the default, All Domains, the base variable is empty, as shown. Otherwise, the base variable is the same as Base DN. See Understanding Base DN.
- Filter: {(&(objectCategory=person)(UserAccountControl:1.2.840.113556.1.4.803:=512)(sAMAccountName=*))(!(userAccountControl:1.2.840.113556.1.4.803:=2))}
  The filter variable depends on the User LDAP filter setting.
- Index used: idx_objectCategory:32561:N
  The search used this index in our testing environment, using a standard AD configuration (no indexes added). Results may be different for a different configuration, especially a different User LDAP filter setting.
- Attributes returned: sAMAccountName, userAccountControl, givenName, sn, [telephoneNumber], [chairpasscode], [confpasscode]
  The three attributes returned variables (in square brackets) are returned only if you specify the corresponding Active Directory attributes (for generating conference room IDs, chairperson passcodes, and conference passcodes, respectively) and if the attribute replication search determined that the attributes are replicated to the global catalog.
**Group Search**

The Group Search queries the global catalog. In a standard AD configuration, all the filter attributes and attributes returned are replicated to the global catalog.

- **Base:** `<empty>`
  
  The base variable depends on the Base DN setting on the Microsoft Active Directory page. If it’s set to the default, All Domains, the base variable is empty, as shown. Otherwise, the base variable is the same as Base DN. See Understanding Base DN.

- **Filter:** `(&(objectClass=group)(|(groupType=-2147483640)(groupType=-2147483646)))`

- **Indexes used:** `idx_groupType:6675:N;idx_groupType:11:N`
  
  The search used these indexes in our testing environment, using a standard AD configuration (no indexes added). Results may be different for a different configuration.

- **Attributes returned:** `cn, description, sAMAccountName, groupType, member`

**Global Group Membership Search**

The Global Group Membership Search queries LDAP.

- **Base:** `DC=dma,DC=eng,DC=local`
  
  The base variable depends on the Base DN setting on the Microsoft Active Directory page. If it’s set to the default, All Domains, the base variable is the domain DN, as shown by the example. Otherwise, the base variable is the same as Base DN. See Understanding Base DN.

- **Filter:** `(&(objectClass=group)(groupType=-2147483646))`

- **Index used:** `idx_groupType:6664:N`
  
  The search used this index in our testing environment, using a standard AD configuration (no indexes added). Results may be different for a different configuration.

- **Attributes returned:** `member`

**Attribute Replication Search**

The Attribute Replication Search queries LDAP.

The system runs this query when it restarts (if already integrated with the Active Directory) and when you click the Update button on the Microsoft Active Directory page, but only if one or more of the configurable Active Directory attributes (for generating conference room IDs, chairperson passcodes, and conference passcodes) is specified.

The purpose of this query is simply to determine if those Active Directory attributes are replicated to the global catalog. If they are, the User Search retrieves them. If any of them is not, the system uses the Configurable Attribute Domain Search to retrieve the data from each domain controller.

- **Base:** `CN=Schema,CN=Configuration,DC=dma,DC=eng,DC=local`
  
  The base variable depends on the forest root.

- **Filter:** `(&(LDAPDisplayName=telephoneNumber)(LDAPDisplayName=chairpasscode)(LDAPDisplayName=confpasscode))`

  The filter variables depend on the configurable Active Directory attributes specified in the Enterprise Conference Room ID Generation and Enterprise Chairperson and Conference Passcode Generation sections (any of these that is empty is omitted from the filter).
Microsoft® Active Directory® Integration

- **Indexes used:** `idx_lDAPDisplayName:3:N; idx_lDAPDisplayName:2:N; idx_lDAPDisplayName:1:N`
- The search used these indexes in our testing environment, using a standard AD configuration (no indexes added). Results may be different for a different configuration.
- **Attributes returned:** `lDAPDisplayName, isMemberOfPartialAttributeSet`

### Configurable Attribute Domain Search

The Configurable Attribute Domain Search queries LDAP.

The system runs this query only if the Attribute Replication Search determined that one or more of the configurable Active Directory attributes that it needs to retrieve (for generating conference room IDs, chairperson passcodes, and conference passcodes) isn’t in the global catalog. In that case, it uses this query to retrieve the data from each domain controller.

- **Base:** `DC=dma,DC=eng,DC=local`
  - The base variable depends on the domain name being queried.
- **Filter:** same as in User Search
- **Index used:** same as in User Search
- **Attributes returned:** `sAMAccountName`, attribute(s) not in global catalog

### Domain Search

The Domain Search queries LDAP.

The system runs this query only when it restarts (if already integrated with the Active Directory) and when you click the **Update** button on the Microsoft Active Directory page.

- **Base:** `CN=Configuration, DC=dma, DC=eng, DC=local`
  - The base variable depends on the forest root DN (the distinguished name of the Active Directory forest root domain).
- **Filter:** `{&(objectCategory=crossRef)(systemFlags=3)}`
- **Indexes used:** `idx_objectCategory:11:N`
  - The search used these indexes in our testing environment, using a standard AD configuration (no indexes added). Results may be different for a different configuration.
- **Attributes returned:** `cn, dnsRoot, nCName`

### Service Account Search

The Service Account Search queries the global catalog. In a standard AD configuration, all the filter attributes and attributes returned are replicated to the global catalog.

The system runs this query only when you click the **Update** button on the Microsoft Active Directory page. It validates the service account ID.

- **Base:** `<empty>`
  - The base variable depends on the **Base DN** setting on the Microsoft Active Directory page. If it’s set to the default, **All Domains**, the base variable is empty, as shown. Otherwise, the base variable is the same as **Base DN**. See Understanding Base DN.
Microsoft® Active Directory® Integration

- **Filter:** 
  \(\& (\text{objectCategory}=\text{person}) \&(\text{UserAccountControl}:1.2.840.113556.1.4.803:512) \&(\text{sAMAccountName}=*)\)
  
  \(\&!((\text{userAccountControl}:1.2.840.113556.1.4.803:2))\)
  
  \(\&(\text{sAMAccountName}=\text{<userID>})\))

  The first filter variable depends on the User LDAP filter setting. The second variable depends on the value entered in the Service account ID field on the Microsoft Active Directory page.

- **Index used:** \text{idx\_objectCategory:32561:N}

  The search used this index in our testing environment, using a standard AD configuration (no indexes added). Results may be different for a different configuration, especially a different User LDAP filter setting.

- **Attributes returned:** \text{sAMAccountName, userAccountControl, givenName, sn}

### View the Active Directory Page

You can view the Microsoft Active Directory page for reference.

**To view the Active Directory page:**

- Go to Integrations > Microsoft Active Directory.

  The following table describes the fields on the Microsoft Active Directory page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrate with Enterprise Directory Server</td>
<td>Enables the Active Directory integration fields and the Update button, which initiates a connection to the Microsoft Active Directory.</td>
</tr>
</tbody>
</table>

**Connection Status**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster</td>
<td>The Polycom RealPresence DMA system server(s) that is integrated with Active Directory.</td>
</tr>
<tr>
<td>Integration Status</td>
<td>Integrated indicates that the server successfully connected to the Active Directory. If it did not, an error message appears.</td>
</tr>
<tr>
<td>User and group cache</td>
<td>Shows the state of the server’s cache of directory data and when it was last updated.</td>
</tr>
<tr>
<td>Refresh duration (seconds)</td>
<td>The duration of the processing of the most recent cache refresh.</td>
</tr>
<tr>
<td>Total users/rooms</td>
<td>Number of enterprise users and enterprise conference rooms in the cache. The difference between the two, if any, is the number of conference room errors.</td>
</tr>
<tr>
<td>Conference room errors</td>
<td>Number of enterprise users for whom conference rooms could not be generated.</td>
</tr>
</tbody>
</table>

**Note:** If you do not specify an Active Directory attribute for conference room ID generation, the number of rooms is zero.

**Note:** If you do not specify an Active Directory attribute for conference room ID generation, the number of errors equals the number of users.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Orphaned groups and users</td>
<td>Number of orphaned users and groups (that is, users and groups that are disabled or no longer in the directory, but for whom the system contains data). If you are an administrator, this label is a link to the Orphaned Groups and Users Report.</td>
</tr>
<tr>
<td>Enterprise passcode errors</td>
<td>Number of enterprise users for whom passcodes were generated that are not valid.</td>
</tr>
</tbody>
</table>

**General Integration Settings**

<table>
<thead>
<tr>
<th>Enterprise Directory Server DNS Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-discover</td>
<td>If this option is selected, the system uses serverless bind to find the closest global catalog servers. Enter the DNS domain name. We strongly recommend using this option. If the system cannot determine the site to which it belongs, it tries to connect to any global catalog server. If that fails, it uses the entered DNS domain name as a host name and continues as if the IP address or host name option were selected. If this option is checked, the system attempts to connect to the Active Directory as follows: 1 It looks up the LDAP servers for the DNS domain (using DNS SRV: _ldap._tcp.&lt;domain-name&gt;). 2 It LDAP-pings every returned LDAP server until one responds with the system's client site name. 3 It looks up the global catalog servers for the site (using DNS SRV: _gc._tcp.&lt;site-name&gt;._sites.&lt;domain-name&gt;). 4 It tries to connect to the global catalog servers. 5 If it can't connect, it tries other global catalog servers from the forest. 6 If it still cannot connect, it uses the DNS domain name (using DNS A: &lt;domain-name&gt;) and connects to it. Step 6 is the system behavior if this option is not checked. The system's network settings must have at least one domain name server specified.</td>
</tr>
<tr>
<td>IP address or FQDN</td>
<td>If this option is selected, the system attempts to connect to the Microsoft Active Directory domain controller specified. For a single-domain forest, enter the host name or IP address of a domain controller. For a multi-domain forest, Polycom does not recommend using this option. If you must, enter the host name or IP address of a specific global catalog server, not the DNS domain name. The RealPresence DMA system can only integrate with one forest. A special &quot;Exchange forest&quot; (in which all users are disabled) will not work because the system does not support conferencing for disabled users.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Domain</td>
<td>The Active Directory domain in which the RealPresence DMA system should create and publish Active Directory contacts. If the system is upgraded from a version prior to 6.2 to version 6.2 or later, the initial value of this field is the Destination network of the SIP Peer configured in Skype pool to create/publish to on the Service Config &gt; Conference Manager Settings &gt; Conference Settings page.</td>
</tr>
</tbody>
</table>
| Domain\Enterprise Directory User ID | LDAP service account user ID for system access to the Active Directory. Must be set up in the Active Directory, but should not have Windows login privileges.  
**Note:** If you use Active Directory attributes that are not replicated across the enterprise via the Global Catalog server mechanism, the system must query each domain for the data. Make sure that this service account can connect to all the LDAP servers in each domain. The Polycom RealPresence DMA system initially assigns the Administrator user role to this user, so you can use this account to give administrative access to other enterprise user accounts.  
**Caution:** Leaving a user role assigned to this account represents a serious security risk. For best security, remove the Administrator user role and mark this account disabled in the Polycom RealPresence DMA system (not the Active Directory) so that it cannot be used for conferencing or for logging into the Polycom RealPresence DMA system management interface. |
| Enterprise Directory User Password | Login password for service account user ID. |
| Security Level | Specifies which user accounts to include (an underlying, non-editable filter excludes all non-user objects in the directory). The default expression includes all users that do not have a status of disabled in the directory. Do not edit this expression unless you understand LDAP filter syntax. See RFC 2254 for syntax information. |
| User LDAP filter | Can be used to restrict the Polycom RealPresence DMA system to work with a subset of the Active Directory (such as one tree of multiple trees, a subtree, or a domain). Leave the default setting of All Domains, initially. |
| Base DN | This is the domain or domain tree to be queried for Active Directory users. Leave the default setting of All Domains, initially. |
| Cache Refresh | The number of cache refreshes per day that the RealPresence DMA system should log in to the directory server(s) and update its cache of user and group data. The time at which the RealPresence DMA system should log into the directory servers and update its cache of user and group data. The time at which the RealPresence DMA system should log into the directory servers and update its cache of user and group data. If the cache is refreshed more than once per day, this will be one of those times (but not necessarily the first time). Specifies the territory whose RealPresence DMA system cluster is responsible for updating the user and group data cache. In a superclustered system, this information is shared across the supercluster. The other clusters access the directory only to authenticate passwords. |
## Microsoft® Active Directory® Integration

### Enterprise Conference Room ID Generation

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Directory attribute         | The name of the Active Directory attribute from which the Polycom RealPresence DMA system should derive conference room IDs (virtual meeting room numbers). Generally, organizations use a phone number field for this.  
The attribute must be in the Active Directory schema and preferably should be replicated across the enterprise via the Global Catalog server mechanism. But if the attribute isn’t in the Global Catalog, the system queries each domain controller for the data.  
Leave this field blank if you do not want the system to create conference rooms for the enterprise users. |
| Characters to remove         | Characters that might need to be stripped from a phone number field’s value to ensure a numeric conference room ID.  
The default string includes \t, which represents the tab character. Use \\ to remove backslash characters.  
If generating alphanumeric conference room IDs, remove the following: ()&%#@"'":;,.  
Single spaces in the source field are preserved, but multiple consecutive spaces are concatenated to one space. |
| Maximum characters used      | Desired length of conference room IDs. The Polycom RealPresence DMA system strips excess characters from the beginning, not the end. If you specify 7, the room IDs will contain the last 7 valid characters from the Active Directory attribute being used.                                                            |

### Enterprise Chairperson and Conference Passcode Generation

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Chairperson directory attribute | The name of the Active Directory attribute that contains the chairperson passcodes. In choosing an attribute, remember that passcodes must be numeric.  
The attribute must be in the Active Directory schema and preferably should be replicated across the enterprise using the Global Catalog server mechanism. But if the attribute is not in the Global Catalog, the system queries each domain controller for the data.  
Leave this field blank if you don’t want the system to create chairperson passcodes for the enterprise users. |
<p>| Maximum characters used      | Desired length of chairperson passcodes. The Polycom RealPresence DMA system strips excess characters from the beginning, not the end. If you specify 7, the passcodes will contain the last 7 numeric characters from the Active Directory attribute being used.                                                            |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conference directory attribute</td>
<td>The name of the Active Directory attribute that contains the conference passcodes. In choosing an attribute, remember that passcodes must be numeric. The attribute must be in the Active Directory schema and preferably should be replicated across the enterprise via the Global Catalog server mechanism. But if the attribute is not in the Global Catalog, the system queries each domain controller for the data. Leave this field blank if you do not want the system to create conference passcodes for the enterprise users.</td>
</tr>
<tr>
<td>Maximum characters used</td>
<td>Desired length of conference passcodes. The Polycom RealPresence DMA system strips excess characters from the beginning, not the end. If you specify 7, the passcodes will contain the last 7 numeric characters from the Active Directory attribute being used.</td>
</tr>
<tr>
<td><strong>Skype RealConnect™</strong></td>
<td></td>
</tr>
<tr>
<td>Callback contacts OU</td>
<td>The OU the system should use for managing Active Directory contacts used for “callbacks”. The feature of hosting RealConnect™ conferences on external Skype systems requires Active Directory contact names to be passed with the signaling between the external Skype system and the Polycom MCU. These contact names enable the external Skype system to “call back” to the Polycom MCU. The RealPresence DMA system manages a pool of these contacts which can be used for this purpose. The system uses all of the contacts that it finds in the specified OU as part of this pool. When the system starts a new conference through the dial rule action <strong>Resolve to Skype Conference ID by Conference Auto Attendant</strong>, it selects an unused contact from the pool and provides the contact name to the Polycom MCU for use in its signaling. Once the conference has ended, the RealPresence DMA system reclaims the contact for reuse. For example: If you create a container for callback contact accounts at the root of your Active Directory domain called “CallbackContacts”, specify: <code>ou=CallbackContacts</code> for this field. If “CallbackContacts” is under the “Development” container, specify: <code>ou=CallbackContacts,ou=Development</code> for this field. For more information on how to configure callback contact accounts in Active Directory, see the Polycom Unified Communications for Microsoft Environments - Solution Deployment Guide. <strong>Note:</strong> Within the Active Directory, all of the callback contacts must exist within the specified OU, and you must enable the setting <strong>Enable for Skype Server</strong> for each contact. You must also ensure that there are enough callback contacts in the OU for the cluster to use under heavy conferencing loads. There can be up to 2400 concurrent RealConnect™ conferences hosted on external Skype systems.</td>
</tr>
</tbody>
</table>
Microsoft Exchange Server Integration

To support Polycom® Conferencing for Microsoft® Outlook®, you can integrate the Polycom RealPresence DMA system with your Microsoft Exchange server. This integration enables users who install the Polycom Conferencing Add-in for Microsoft Outlook to set up Polycom Conferencing meetings in Outlook.

When you integrate the RealPresence DMA system with an Exchange server, it connects to the Exchange server as the Polycom Conferencing user and subscribes to notifications. The Exchange server notifies the RealPresence DMA system as soon as a meeting invitation (or other mail) arrives in the Polycom Conferencing user Inbox. It also sends heartbeat messages to verify that the subscription is working.

If the RealPresence DMA system fails to receive a heartbeat or other notification for 30 seconds, it begins checking its Inbox every four minutes for new messages, and also attempts to reestablish the subscription (push connection) each time.

As with other Outlook meeting requests, the meeting organizer invites attendees and specifies where and when to meet. “Where” in this case is a conference room, or virtual meeting room (VMR), on the RealPresence DMA system. The VMR number is generated by the add-in.

The invitees may include conference-room-based Polycom HDX systems as well as users with Polycom HDX personal conferencing endpoints. Polycom HDX systems monitor an Exchange mailbox (either their own or a linked user’s) for Polycom Conferencing meeting invitations.

Invitees with a desktop conferencing client (such as Polycom® RealPresence® Desktop) can join the meeting by clicking a link in the Outlook reminder or calendar. Invitees with a Polycom HDX endpoint can join by clicking a link on the HDX system’s reminder.

The add-in also sends Polycom Conferencing meeting invitations to a Polycom Conferencing user mailbox on the Exchange server. The RealPresence DMA system accepts or declines these invitations. A meeting invitation is declined if:

- The VMR number is in use by any other conference room (calendared, enterprise, or custom).
- The user sending the invitation is not in the Polycom RealPresence DMA system’s Active Directory cache.
- The invitation contains invalid or incomplete meeting data (the machine-readable metadata block at the bottom of the invitation labeled “POLYCOM VMR ENCODED TOKEN” and preceded with a warning not to edit).
- The meeting’s duration exceeds the system’s Default Conference Duration setting.
- The conference or chairperson passcode is not valid.

Polycom Solution and Integration Support

Polycom Implementation and Maintenance services provide support for Polycom solution components only. Additional services for supported third-party Unified Communications (UC) environments integrated with Polycom solutions are available from Polycom Global Services, and its certified Partners, to help customers
Microsoft Exchange Server Integration

successfully design, deploy, optimize, and manage Polycom visual communication within their third-party UC environments. Polycom Collaboration Services for Microsoft integration are mandatory for Polycom Conferencing for Microsoft Outlook and Microsoft Office Communications Server integrations. See http://www.polycom.com/services/professional_services/index.html or contact your local Polycom representative for more information.

Differences Between Calendaring and Scheduling

Calendaring is not the same as scheduling. Using the Polycom Conferencing Add-in for Microsoft Outlook to set up a meeting appointment does not reserve video resources, and invitations are not declined due to lack of resources.

The Polycom RealPresence DMA system supports the use of Cisco Codian 4200, 4500, and MSE 8000 series MCUs as part of its conferencing resource pool. If you use Codian MCUs to host Polycom Conferencing (calendared) meetings, be aware of these limitations:

- Codian MCUs do not support the Polycom Conferencing Add-in’s recording and streaming options.
- Codian MCUs do not provide the “gathering phase” that RMX and RealPresence Collaboration Server MCUs provide at the beginning of the conference.

Codian MCUs cannot receive and accept Outlook meeting invitations themselves, and can only be used if a RealPresence DMA system is part of the Polycom Conferencing for Outlook solution.

Microsoft Exchange Server Page

The following table describes the fields on the Microsoft Exchange Server page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable integration with Microsoft® Exchange Server</td>
<td>Enables the Exchange server integration fields and the Update button, which initiates a connection to Microsoft Exchange server.</td>
</tr>
<tr>
<td>Exchange Server address</td>
<td>Fully Qualified Domain Name (FQDN) or IP address of the Exchange server.</td>
</tr>
<tr>
<td>Domain/user name</td>
<td>The user ID for the Polycom Conferencing infrastructure mailbox on the Exchange server.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for the Polycom Conferencing user ID.</td>
</tr>
<tr>
<td>Territory</td>
<td>Select a territory, thereby determining which Polycom RealPresence DMA cluster is responsible for integrating with the Exchange server and monitoring the Polycom Conferencing infrastructure mailbox.</td>
</tr>
<tr>
<td>Accept Exchange notifications from these additional IP addresses</td>
<td>If you have multiple Exchange servers behind a load balancer, specify the IP address of each individual Exchange server.</td>
</tr>
</tbody>
</table>

Exchange Server Integration

Unless the Allow unencrypted calendar notifications from Exchange server security option is enabled (see Security Settings), the RealPresence DMA system offers the same SSL server certificate that it offers
Microsoft Exchange Server Integration

to browsers connecting to the system management interface. The Exchange server must be configured to trust the certificate authority in order for the RealPresence DMA system to subscribe to notifications.

If the RealPresence DMA system is configured with a self-signed certificate and the **Allow unencrypted calendar notifications from Exchange server** security option is disabled, Exchange server integration will fail.

If the RealPresence DMA system is unable to subscribe to notifications, the Exchange Server status (see Dashboard) remains **Subscription pending** indefinitely and the RealPresence DMA system does not automatically receive calendar notifications. Instead, it must check the Polycom Conferencing mailbox for meeting request messages, which it does every 4 minutes.

**Integrate the Polycom RealPresence DMA System with Your Exchange Server**

To enable Polycom Conferencing for Microsoft Outlook, you need to integrate the RealPresence DMA system with your Exchange server.

Before integrating with your Exchange server, ensure that the RealPresence DMA system is integrated with Microsoft Active Directory.

To integrate the Polycom RealPresence DMA system with your Exchange server:

1. Confirm that the RealPresence DMA system has been successfully integrated with your Active Directory and verify the domain.
2. Ensure that the DNS server used by the Microsoft Exchange server (usually, the nearest Active Directory domain controller) has an A record for the RealPresence DMA system that resolves the system’s FQDN to its virtual IP address.
3. On the Microsoft Exchange server, create the Polycom Conferencing user that the add-in will automatically invite to Polycom Conferencing meetings.
   1. For the user ID, specify the same domain used to integrate with the Active Directory.
   2. Enter the Display Name as you want it to appear in the **To** field of invitations, for example, Polycom Conference (first and last name).
4. Go to **Integrations > Microsoft Exchange Server**.
5. Check **Enable integration with Microsoft® Exchange Server** and specify the address (host name or IP address) of the Exchange server.
6. Specify the login credentials for the system on the Exchange server.
7. Set **Territory** to the territory of the Polycom RealPresence DMA cluster to be responsible for calendaring.
8. If you have multiple Exchange servers behind a load balancer, under **Accept Exchange notifications from these additional IP addresses**, add the IP address of each individual Exchange server.
9. Click **Update**.
   A dialog informs you that the configuration has been updated.
10. Click **OK**.
11 Install the Polycom Conferencing Add-in for Microsoft Outlook on your PC and create the configuration to be distributed to your users (see the online help for the Add-in). Optionally, customize the invitation template(s).

12 Distribute the Polycom Conferencing Add-in for Microsoft Outlook, its configuration file, and customized templates to your users (see the System Administrator Guide for the Polycom® Conferencing Add-in for Microsoft® Outlook®).
Microsoft® Skype® for Business Integration

The RealPresence DMA system allows you to integrate with Microsoft® Skype® for Business 2015 Standard Edition and Enterprise Edition environments. When you integrate the RealPresence DMA system into a Skype for Business environment, the system communicates with the Skype servers and Active Directory to provide contact presence and conference interaction between MCUs managed by the RealPresence DMA system and the Skype for Business AVMCU. Presence allows Skype clients to view the presence of a RealPresence DMA system VMR, similar to any other contact in the Skype client contact list.

The RealPresence DMA system may also be integrated with Lync 2013 if you have not yet upgraded your environment to Skype for Business.

**Note:** Throughout this guide, the term “Polycom conference contact” is used to refer to an Active Directory contact that corresponds with a VMR on the RealPresence DMA system and allows Skype presence status to be published for that VMR. You can configure the RealPresence DMA system to create and delete Polycom conference contacts automatically.

Callers can also connect to a conference containing a mixture of Skype clients and other endpoints.

The following topics describe integration with Skype for Business:

- Lync 2013 vs. Skype for Business 2015 Integration
- Scheduled Conferences with Polycom RealConnect™
- Automatic Contact Creation and Configuration
- Active Directory Service Account Permissions
- Skype and non-Skype Endpoint Collaboration
- Considerations and Requirements for Integration with Skype for Business 2015
- Lync 2010 and 2013 Client / Server Feature Support
- Integrate RealPresence DMA and Skype for Business 2015
- Diagnose Presence Problems

**Lync 2013 vs. Skype for Business 2015 Integration**

The RealPresence DMA system can interact with both Lync 2013 and Skype for Business 2015 environments. However, there are some differences between interacting with a Lync 2013 environment and full integration with a Skype for Business 2015 environment.

When the RealPresence DMA system is integrated with Lync 2013, Lync clients that connect to RealPresence DMA system VMRs may be hosted on the Lync AVMCU, and can be part of RealPresence DMA system conferences via a cascade link that the Polycom MCU creates with the AVMCU.
Integration also allows a non-Lync client to connect to a Lync 2013 scheduled conference by dialing the Lync conference ID included in the Microsoft Outlook meeting invitation. The RealPresence DMA system receives the connection attempt, creates a matching VMR automatically, and builds a cascade link between a Polycom MCU and the Lync AVMCU.

When the RealPresence DMA system is integrated with Skype for Business 2015, conferencing connections for Skype and non-Skype clients function as described for Lync 2013. However, Polycom RealConnect™ conferences with Lync 2013 and Skype for Business 2015 Server (on premise) also benefit from Skype MCU affinity.

Skype for Business deployments can be geographically distributed. When you use Polycom RealConnect™ technology, video conferences can occur on various Skype AVMCUs deployed throughout the geography. Skype MCU affinity enables the RealPresence DMA system to select a Polycom MCU in proximity to the Skype AVMCU hosting the Polycom RealConnect™ conference. This capability can reduce call latency, traffic, and costs.

Scheduled Conferences with Polycom RealConnect™

The Polycom RealConnect™ scheduled conference scenario is a single workflow for scheduling conferences for Skype and non-Skype endpoints. Once you integrate your system with a Skype for Business 2015 environment, registered endpoints can call through the RealPresence DMA system and join conferences that you schedule with Microsoft Outlook. The Polycom Conferencing for Outlook (PCO) plugin is not needed for Polycom RealConnect.

Note: Polycom RealConnect-scheduled conferences require that the RealPresence DMA system manage at least one Polycom MCU that supports Skype for Business 2015. Non-Polycom MCUs are not supported.

Polycom RealConnect uses Microsoft Outlook meeting invitations to deliver conference information to participants. When you schedule a conference with Outlook, you can configure the Outlook meeting invitation to include Skype conference IDs as plain text, in addition to the automatically included “Join Skype Meeting” hypertext link. When they receive the meeting invitation, users of Skype clients can click the link, and users of non-Skype endpoints can dial the plain-text Skype conference ID.

When non-Skype endpoints dial the meeting ID in the meeting invitation, the RealPresence DMA system responds to the incoming call by applying a dial rule with the action Resolve to Skype conference ID. This dial rule prompts the RealPresence DMA system to search any of the dial rule’s configured and selected SIP peers (representing Skype front-end pools) for a matching Skype conference. If the meeting ID isn’t resolved on one of the selected SIP peers, the system continues to attempt to resolve the dial string using the next dial rule in the list.

If the conference ID is resolved on one of the selected SIP peers, the SIP peer gives the RealPresence DMA system the focus URI of the conference. From this information, the RealPresence DMA system extracts Skype user information, then queries the Skype for Business deployment to obtain the FQDN of the front-end pool which hosts the AVMCU conference. Once the RealPresence DMA system receives a response, it searches the selected SIP peers in the dial rule for a next hop address that matches the front-end pool FQDN. When the system finds a match, it uses the MCU pool order configured in the matching external SIP peer to select the MCU to host the conference. The RealPresence DMA system dynamically creates a VMR and, using the configured MCU pool order, starts a conference on a Polycom MCU in proximity to the Skype AVMCU that is hosting the Polycom RealConnect™ conference. Using the Skype focus URI received from the RealPresence DMA system, the MCU builds a cascade link between
the newly created conference and the Skype AVMCU. Skype clients and non-Skype endpoints can now interact in the conference. If there is no selected SIP peer with a matching FQDN, or if the matching SIP peer does not have a configured MCU pool order, the RealPresence DMA system uses the MCU pool order configured in the dial rule.

In a superclustered configuration, endpoints can connect to a RealConnect™ conference from any cluster in the supercluster, but the call will be routed through the supercluster to the cluster that is hosting the RealConnect™ conference.

If the RealPresence DMA system loses connection with a Skype server, the system tries to reconnect and alerts the administrator of the outage.

For information on configuring Microsoft Outlook and Microsoft Skype for Business 2015 to support Polycom RealConnect™, refer to the Polycom Unified Communications for Microsoft Environments - Solution Deployment Guide.

**Automatic Contact Creation and Configuration**

You can configure the RealPresence DMA system to create and manage a corresponding Polycom conference contact in Active Directory whenever users create a new VMR. The RealPresence DMA system communicates with the Skype server to ensure the new contact is enabled for Skype functionality. This allows the system to publish presence updates to the conference contact; Skype clients display a status of Available, Busy, or Offline for the conference contact in the client's contact list.

*Note:* When you manually or automatically create a VMR or group of VMRs, allow up to 10 minutes for the newly created conference contact(s) to appear in the Skype client contact list.

**Active Directory Service Account Permissions**

If you integrate the RealPresence DMA system with Skype for Business 2015 and plan to use the automatic conference contact creation feature, note that the required Active Directory service account should have full permissions to add, change, and delete entries in the OU where the conference contacts are stored. The account should also have full administrative permissions for Skype administration to manipulate these contacts.

**Skype and non-Skype Endpoint Collaboration**

Callers with Skype clients and non-Skype endpoints can join the same conference in several ways. See the Microsoft Skype for Business documentation for more details on specific call flows.

- Users of Skype clients can select a Polycom conference contact in the contact list and drag it to an ongoing Skype conversation window, starting a video call.
- Users of Skype clients can start a Skype conference by selecting the **Show Menu** icon and choosing **Meet Now**. After starting the conference, users can invite more attendees to the conference or drag a Polycom conference contact into the conversation window to add the participant.
- Users of Skype clients can right-click a Polycom conference contact in the contact list and choose **Start a video call**.
Users of Skype clients and other endpoints can use a Microsoft Outlook meeting invitation to connect to a Skype conference. Non-Skype endpoints can dial the included conference ID, and Skype clients can click the “Join Skype Meeting” link included in the invitation.

When you register a Polycom endpoint to a RealPresence DMA system and make a point-to-point call to a Lync 2013 or Skype for Business 2015 client, the conference may not have video because the H.261 and H.263 video codecs are not supported by the Lync or Skype client. As a workaround for Polycom HDX and RealPresence Group Series endpoints, register the endpoint to the Lync or Skype server before starting the conference. This workaround requires an RTV option key or Lync/Skype Interoperability License.

If you add a SIP endpoint on the Network > Endpoints page using the Address of record format `<name>@<IP address>` and call the endpoint using a Lync 2010 client, the endpoint will not hang up when the call is terminated from the Lync 2010 client. As a workaround, use an Address of record with the format `<name>@<SIP domain>` when adding the endpoint.

Considerations and Requirements for Integration with Skype for Business 2015

For the latest software version requirements and interoperability information, consult the Polycom Unified Communications in a Microsoft Environment Release Notes.

The following Virtual Entry Queue (VEQ) call scenarios are not supported:
- Calls to a Virtual Entry Queue (VEQ) from a Skype client
- A non-Skype endpoint connecting to a VEQ and entering a Skype conference ID when prompted

Conference mode configurations of SVC-only and Mixed AVC and SVC are not supported in RealPresence DMA system and Skype cascaded conferences. Any conference that requires Skype AVMCU connectivity must use conference templates with AVC only as the configured Conference mode.

You need Skype-capable Polycom MCUs to take advantage of Polycom RealConnect™ functionality. Non-Polycom MCUs are not supported. If your Polycom MCU is Skype-capable, the icon is displayed next to the MCU name on the Integrations > MCU page. If no MCUs that support Skype for Business are available, the cascaded RealConnect™ conference won't start. Refer to your MCU documentation for more information.

The Transfer Call feature of the Lync or Skype client is currently not supported when the MCU hosting the call is configured to use ICE or encryption.
## Lync 2010 and 2013 Client / Server Feature Support

The following table outlines features that the RealPresence DMA system supports in Lync 2010 and Lync 2013 client and server environments.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Client</th>
<th>Server</th>
<th>Uses SVC cascading between Microsoft AVMCU and Polycom MCU</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduling - Dial to RealConnect™ conference</td>
<td>Lync 2013</td>
<td>Lync 2013</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Skype 2015</td>
<td>Skype 2015</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multipoint Lync conferences invite a VMR</td>
<td>Lync 2013</td>
<td>Lync 2013</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Skype 2015</td>
<td>Skype 2015</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Meet Now calls to a VMR</td>
<td>Lync 2013</td>
<td>Lync 2013</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Skype 2015</td>
<td>Skype 2015</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Escalated conferences - Lync client drag and drop multi-party call</td>
<td>Lync 2013</td>
<td>Lync 2013</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Skype 2015</td>
<td>Skype 2015</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct point-to-point Lync call to a VMR</td>
<td>Lync 2010</td>
<td>Lync 2010</td>
<td>No</td>
<td>If a Lync 2013 client, all calls will be audio only.*</td>
</tr>
<tr>
<td></td>
<td>Lync 2013</td>
<td>Lync 2013</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DMA registered endpoint calling point to point to a Lync client</td>
<td>Lync 2010</td>
<td>Lync 2010</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lync 2013</td>
<td>Lync 2013</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lync client calling point to point to DMA registered endpoint</td>
<td>Lync 2010</td>
<td>Lync 2010</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lync 2013</td>
<td>Lync 2013</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Presence enabled VMRs</td>
<td>Lync 2013</td>
<td>Lync 2013</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

* The Lync 2010 client supports the H.263 video codec, but the Lync 2013 client does not. See Skype and non-Skype Endpoint Collaboration.
Integrate RealPresence DMA and Skype for Business 2015

Refer to the Polycom Unified Communications for Microsoft Environments - Solution Deployment Guide for the tasks needed to integrate the RealPresence DMA system with Skype for Business 2015. If you need the RealPresence DMA system to automatically create conference contacts in Active Directory, ensure that your system is integrated with Microsoft Active Directory before proceeding.

Diagnose Presence Problems

If after integration your Skype client does not display presence for RealPresence DMA system VMRs when you enable automatic contact creation and presence publishing, use the following points to begin troubleshooting.

- Check for any active system alerts
  The description of any active system alerts can indicate potential issues with integration. See the online help or the Polycom RealPresence DMA System Operations Guide for a description of the alert text.

- Verify NTP Lync server and RealPresence DMA system use the same NTP source
  If the system time differs slightly between the RealPresence DMA system and the Skype server, the Skype server can reject contact creation attempts. See the Admin > Server > Time Settings page to configure NTP servers.

- Ensure supported MCUs are in service with available ports
  See the Integrations > MCU page for an overview of MCU status.

- Ensure that the Publish presence for Polycom conference contacts check box is enabled
  This setting, on the Service Config > Conference Manager Settings > Conference Settings page, controls system-wide presence publishing for conference contacts.
RealPresence Resource Manager Integration

Integrating with a RealPresence Resource Manager system provides the RealPresence DMA system with the following information:

- All site topology information configured in the RealPresence Resource Manager system.
  The Polycom RealPresence DMA system uses site topology information for a variety of purposes, including cascade for bandwidth conferences, bandwidth management, and Session Border Controller selection.

- All user-to-device associations configured in the RealPresence Resource Manager system in which the enterprise user is also known to the RealPresence DMA system.
  The RealPresence DMA system uses user-to-device associations to assign classes of service to endpoints based on the user they belong to.

  Note: The RealPresence DMA system currently does not support integration with a Polycom RealPresence Resource Manager system when the RealPresence DMA system is configured for split network interfaces.

Integrating with a RealPresence Resource Manager system allows you to configure site topology and user-to-device associations in one place instead of two, ensuring consistency. While integrated, you can configure this information only in the RealPresence Resource Manager system. If you do not have a RealPresence Resource Manager system, or if the RealPresence DMA system and RealPresence Resource Manager system are not integrated, both kinds of information can be manually configured in the RealPresence DMA system. If the integration is terminated, the RealPresence DMA system retains the information last obtained from the RealPresence Resource Manager system and it becomes editable.

When the RealPresence DMA system gets its site topology from a RealPresence Resource Manager system, the first three territories assigned to a RealPresence DMA cluster are enabled for conference rooms.

The **Bit rate to bandwidth conversion factor** setting on the **Call Server Settings** page of the RealPresence DMA system can affect choices for bandwidth restrictions in your site topology. Since the RealPresence Resource Manager system calculates call bandwidth requirements using a conversion factor of 2.5, Polycom recommends using a **Bit rate to bandwidth conversion factor** value of 2.5 if you integrate with a RealPresence Resource Manager system. Otherwise, you will need to alter the bandwidth restrictions for your site topology to take into account the conversion factor value so that the RealPresence DMA system's call bandwidth requirement calculations are predictable.
Considerations When Integrating with a RealPresence Resource Manager System

When integrating a RealPresence Resource Manager system with the RealPresence DMA system, be aware of the following considerations:

- When you integrate the Polycom RealPresence Resource Manager system to a RealPresence DMA supercluster with embedded DNS enabled, in the RealPresence Resource Manager’s Add DMA dialog, select **Support DMA Supercluster**.

- Integrating a RealPresence Resource Manager system to a RealPresence DMA system enables the RealPresence Resource Manager system to use the RealPresence DMA system’s RealPresence Platform API to set up and monitor scheduled and preset dial-out (anytime) conferences using the RealPresence DMA system’s resources.

- DNS servers must be able to resolve the RealPresence DMA system’s FQDN to its IP address. In addition, the DNS servers must be able to resolve the RealPresence Resource Manager system’s FQDN to its IP address.

- If the **Allow delegated authentication to enterprise directory server** option on the RealPresence Resource Manager system is not configured and working properly, the RealPresence DMA system does not receive user-to-device association data for enterprise users and intermittently generates alert 2001.

- If you plan to configure two RealPresence DMA nodes as a High Availability pair, configure the network settings and enable and configure the High Availability settings before you integrate with a RealPresence Resource Manager system.

Integrate with a RealPresence Resource Manager System

You can integrate the RealPresence DMA system with a RealPresence Resource Manager system from the **Network Device > DMA** page of the RealPresence Resource Manager management interface.

View RealPresence Resource Manager Integration Details

When your RealPresence DMA system is integrated with a RealPresence Resource Manager system, you can view details about the integration from the RealPresence DMA system.

To view RealPresence Resource Manager integration details:

- Go to **Integrations > RealPresence Resource Manager**.

  The **RealPresence Resource Manager Integration Details** display. The following table describes the fields in the list:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>Name of the system.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the system.</td>
</tr>
<tr>
<td>Version</td>
<td>Software version of the system.</td>
</tr>
</tbody>
</table>
Terminate RealPresence Resource Manager Integration

When the RealPresence DMA system is integrated with a RealPresence Resource Manager system, the RealPresence Resource Manager page contains the Leave RealPresence Resource Manager command, which you can use to terminate the integration. You cannot use this page to integrate with a RealPresence Resource Manager system.

To terminate integration with a RealPresence Resource Manager system:

1. Go to Integrations > RealPresence Resource Manager.
3. When asked to confirm that you want to leave, click Yes.
   The system connects to the RealPresence Resource Manager system, terminates the integration, and informs you when the process is complete.
4. On the RealPresence Resource Manager page, verify that the RealPresence DMA system is no longer integrated with the RealPresence Resource Manager system.
   The RealPresence DMA system retains the site topology and user-to-device association information last obtained from the RealPresence Resource Manager system and it is now editable.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Status of last attempt to contact system (OK or Unreachable).</td>
</tr>
<tr>
<td>Time</td>
<td>Time of last attempt to contact system.</td>
</tr>
</tbody>
</table>
Conference Manager Configuration

This section provides an introduction to configuring conferences hosted by the Polycom® RealPresence® DMA® system. It includes:

- Conference Settings
- Conference Templates
- IVR Prompt Sets
- Shared Number Dialing
Conference Settings

Conference Settings define the default class of service and bit rate limits, a dialing prefix, and various default conference properties for the Polycom® RealPresence® DMA® system. If the system is integrated with a Microsoft® Lync® 2013 or Skype® for Business environment, you can also configure system-wide default settings related to presence publishing for Polycom conference contacts.

Class of Service Overview

You can specify a default class of service when you configure conference settings. Class of service determines the priority of a device in a point-to-point call or the priority of the devices connected to a VMR (conference room), from bronze (lowest priority) to gold (highest priority).

The class of service of a user or group determines the class of service of an associated device. The class of service of a device determines the priority of that device’s point-to-point call. Devices connected to a VMR inherit the class of service of the conference room for the duration of the call.

For example, if your device is assigned a bronze class of service and you attempt to dial a point-to-point call using a RealPresence DMA system saturated with gold- and silver-level conferences, the RealPresence DMA system will reject your call. However, if you use a device with a gold class of service to dial the same point-to-point call using the same RealPresence DMA system, the RealPresence DMA system will disconnect one of the silver-level devices to make room for your device.

Note: The Default maximum bit rate and Default minimum downspeed bit rate are the default values for point-to-point calls and conference room (VMR) calls.

Configure Conference Settings

Conference settings define the default conference properties for the Polycom RealPresence DMA system.

To configure conference settings:

1. Go to Service Config > Conference Manager Settings > Conference Settings.
2. Complete the fields described in the following table as needed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dialing prefix</td>
<td>Numeric dial string prefix for calling VMRs and VEQs. If you specify a prefix, the system uses it for both SIP and H.323 calls so that the same number can be dialed from both H.323 and SIP endpoints. If neighboring with a Polycom gatekeeper on which the Simplified Dialing service is enabled and uses a prefix of 9 (the default), do not use 90-99. The neighbor gatekeeper recognizes the 9 as a known prefix and ignores the second digit. <strong>Caution:</strong> Changing the dialing prefix terminates any existing H.323 calls.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Conference Defaults</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Default class of service</td>
<td>The class of service assigned to a user or endpoint if the class of service is not specified at the endpoint, user, or group level. <strong>Note:</strong> The class of service of the device applies to point-to-point calls. VMR calls use the class of service of the conference room.</td>
</tr>
<tr>
<td>Default maximum bit rate (kbps)</td>
<td>The maximum bit rate for a call if the maximum bit rate for the user or endpoint is not specified at the endpoint, user, or group level.</td>
</tr>
<tr>
<td>Default minimum downspeed bit rate (kbps)</td>
<td>The minimum bit rate to which a call can be reduced (downspeeded) if the minimum downspeed for the user or endpoint is not specified at the endpoint, user, or group level.</td>
</tr>
<tr>
<td>Default max total participants</td>
<td>Specifies the maximum conference size assigned to a conference room. <strong>Automatic</strong> (the default setting) uses the largest conference size supported by the MCU (or by all available MCUs if cascading is enabled) as the default maximum.</td>
</tr>
</tbody>
</table>

| Default conference template   | Default template used by the system.                                                                                                           |
| Default MCU pool order       | Default MCU pool order used by the system.                                                                                                     |
| Default MCU selection algorithm | The process that the RealPresence DMA system uses when it selects MCUs from MCU pool orders: **Prefer MCU in first MCU pool** ensures that the DMA system always routes the call to the first available MCU in the first MCU pool. If no MCU is available, the system searches the second MCU pool for an available MCU, and so on. **Prefer MCU in first caller’s site** matches the MCU chosen for the call with the site to which the first caller’s endpoint belongs. |

<p>| Default conference room territory | The territory assigned to a user’s conference room if it is not specified at the user or conference room level. A conference room’s territory assignment determines which RealPresence DMA cluster hosts the conference (the primary cluster for the territory, or its backup cluster if necessary). Up to three territories in a superclustered system can host conference rooms. |
| Default conference duration    | Default maximum duration of a conference (in hours and minutes) or <strong>Unlimited</strong> (the maximum in this case depends on the MCU).                                                                 |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generated conference room IDs</td>
<td>The minimum and maximum values for auto-generated room IDs created for custom conference rooms. Values may be up to 18 digits long. The 18-digit limit applies only to generated IDs for custom conference rooms.</td>
</tr>
<tr>
<td>Generated conference room aliases</td>
<td>The minimum and maximum values for auto-generated conference room aliases created for custom conference rooms. Values may be up to 18 digits long. The 18-digit limit applies only to conference room aliases for custom conference rooms.</td>
</tr>
<tr>
<td>Generated transient conference IDs</td>
<td>The minimum and maximum values for auto-generated transient conference IDs created for SIP conference factory conferences. Values may be up to 18 digits long. The 18-digit limit applies only to generated conference factory IDs for custom conference rooms.</td>
</tr>
</tbody>
</table>

### MCU Selection Thresholds

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum CIF ports required to start a conference on an MCU</td>
<td>The minimum number of available Common Intermediate Format (CIF) video ports on an MCU that are required for the RealPresence DMA system to start a conference on the MCU.</td>
</tr>
<tr>
<td>Maximum percentage of CIF ports in use to start a conference on an MCU</td>
<td>The maximum percentage of CIF ports already in use on an MCU that determines if the RealPresence DMA system will start a conference on the MCU. The system will not start a conference on an MCU if its percentage of ports already in use is equal to or above the maximum percentage you specify.</td>
</tr>
</tbody>
</table>

### Skype Experience

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Roster cascade indicator     | For Polycom conferences that cascade to Skype conferences, this setting specifies the name that displays in the Skype for Business client as the conference roster entry that corresponds to the Polycom conference. This setting confirms to the Skype client that a participant is valid and belongs in the conference (and should not be deleted). The value is 0-64 characters and can include the following:  
  • upper and lower case letters  
  • spaces  
  • ! % + - _  
  If the field is blank, the system uses conference-ID@domain, where the conference-ID is either the VMR or the Skype conference-ID (for RealConnect conferences). |
### AS SIP settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default resource priority namespace</td>
<td>In an Assured Services SIP (AS-SIP) environment, a Local Session Controller (LSC) can provide priority-based precedence and preemption services to ensure that the most important calls get through. If your organization has implemented such a resource prioritization mechanism, set this value to the namespace being used for resource priority values. If the namespace being used is not listed, select <strong>Custom</strong> and enter the name in the box to the right of the list.</td>
</tr>
<tr>
<td>Default resource priority value</td>
<td>If your organization has implemented a resource prioritization mechanism, set this to the default priority value assigned to a conference if the specific conference room (VMR) does not have a higher value. If using a custom namespace, enter the value in the box to the right of the list.</td>
</tr>
</tbody>
</table>

3. Click **Update** to save the settings.
Conference Templates

Conference templates are used to create users’ conference rooms, which define a user’s conference experience. A conference template specifies a set of conference properties, such as the line (bit) rate and video display mode.

The following conference template topics provide additional information:

- Two Types of Templates
- Template Priority
- About Conference IVR Services
- About Cascading
- WebRTC Conferencing
- View the Conference Templates List
- Add a Conference Template
- Edit a Conference Template
- Select a Video Frames Layout
- Working with Conference Templates

Two Types of Templates

You can create a conference template in two ways:

- Specify the individual conference properties directly in the Polycom RealPresence DMA system, creating a standalone template independent of the profiles available on the system’s Polycom MCUs.
- Link the template to a Polycom MCU conference profile that exists on some or all of the MCUs.

Either type of template can also include settings specific to Cisco Codian MCUs for deployments that include both Polycom MCUs and Cisco Codian MCUs.

Standalone Templates

Standalone templates that you define in the Polycom RealPresence DMA system prevent you from having to ensure that the exact same MCU conference profiles exist on all MCUs. You specify the desired conference properties directly in the template.

When the RealPresence DMA system uses a standalone template for a conference, the system sends the specific properties to the MCU instead of pointing to one of the MCU’s conference profiles.

When using a template not linked to a Polycom MCU conference profile, the RealPresence DMA system does not use the template’s properties to limit its choice of an MCU. It selects the least used MCU in the selected MCU pool. Unsupported properties are ignored or degrade gracefully if necessary. For instance:
● If a conference set to a 4096 kbps line rate is forced to land on an MCU that does not support that value, the line rate falls back to 1920 kbps.

● If a conference with encryption enabled is forced to land on an MCU that does not support encryption, that property is ignored.

To preferentially route conferences to certain MCUs, use MCU pool orders.

**Templates Linked to Polycom MCU Conference Profiles**

Linking a template to a Polycom MCU conference profile lets you access profile properties that are not currently available in a standalone template, as the MCU may offer more conference profile properties than standalone templates. When you link a template with an MCU conference profile, the MCU’s conference profile settings take priority over values set in the RealPresence DMA system template.

When you link a template to a conference profile, consider the following details:

● You must ensure that the conference profile exists on the MCUs you want to use with that template and that the profile’s settings are the same on all of the MCUs.

● If the Polycom MCU conference profile has recording enabled, the RealPresence DMA system does not recognize this and rejects attempts to start recording via the API. To enable recording control via the API, use a standalone conference template with recording enabled.

● When you link to a Polycom MCU conference profile that uses an Interactive Voice Response (IVR) service which does not prompt for passcodes, callers are not prompted even if the conference has a conference or chairperson passcode.

When the RealPresence DMA system uses a profile-based template, the system first tries to find an MCU that has that profile (using the MCU pool order rules). The system selects the least used MCU in the pool that has that profile.

If none of the MCUs in the pool have that profile, the system selects the least used MCU in the pool and does one of the following:

● If the system selected a Cisco Codian MCU, it uses the Codian-specific settings of the specified template.

● If the system selected a Polycom MCU, it falls back to its default conference template (see Conference Settings). If the default template happens to be linked to a profile that this MCU doesn't have, the system falls back to its built-in conference properties settings.

**Template Priority**

A user (local or enterprise) has one or more conference rooms. Each room may either use the system’s default template (specified on the Conference Settings page) or use a specifically assigned template. (Typically, most conference rooms use the default template.)

An enterprise user can be associated with multiple enterprise groups, and each group may or may not have a specifically assigned template.

You can rank the conference templates by priority, so that the system knows which template to use when the user is associated with more than one.

When someone dials into a conference room, the system uses the following rules (in order of importance) to determine which template to use for the conference:

1. If the conference room has a specifically assigned template (not the system default), use that template.
2. If the user associated with the conference room belongs to one or more enterprise groups that have specifically assigned templates, use the template with the highest priority.

3. Otherwise, use the system default conference template.

About Conference IVR Services

In a template, you can optionally specify the conference Interactive Voice Response (IVR) service that the Polycom MCU should use. However, this is not recommended. Polycom MCUs have two defaults, one for conferences with passcodes and one for conferences without passcodes. For conferences configured via the RealPresence DMA system (not linked to a profile), the MCU automatically uses the correct default IVR service for each conference.

If you do choose to override the default and specify an IVR service, the IVR service you select must be appropriate for the users whose conferences will use this template, and it must be available on the MCUs on which those conference may take place. See your Polycom MCU documentation for information about conference IVR services. This feature is not supported on Cisco Codian MCUs.

When you add or edit a conference template, the Polycom MCU Conference IVR tab contains a list of names of all the conference IVR services available on the currently connected MCUs. If an IVR service is only available on some of the connected MCUs, its entry shows how many of the MCUs have that IVR service (for instance, 2 of 3). If a template specifies a conference IVR service, the system will put conferences using that template on the least used MCU that has that conference IVR service. If there are none, it falls back to the default conference IVR service.

Note: Callers to conferences with passcodes (PINs) can bypass the IVR service’s passcode prompting by appending the passcode to the dial string, following the protocol-appropriate delimiter:

- H.323: <vmr number>#<passcode>
- SIP: <vmr number>**<passcode>

About Cascading

One of the conference features you can optionally enable in a template is cascading, which enables a conference to span multiple Polycom MCUs. One of two mutually exclusive forms of cascading can be enabled:

- Cascading for Bandwidth
- Cascading for Size

The cascade links between MCUs use H.323 or SIP signaling. SIP signaling is used in the following situations:

- when the conference is limited to SVC endpoints, or
- one of the MCUs does not support H.323, or
- the conference template settings specify to Cascade for SVC.
Cascading for Bandwidth

Cascading for bandwidth uses a hub-and-spoke configuration; each cascaded MCU is only one link away from the “hub” MCU that hosts the conference. To host the conference, the RealPresence DMA system chooses the same MCU that it would have chosen in the absence of cascading.

Cascading a conference across multiple MCUs to conserve bandwidth is especially useful when using WAN links. Participants can connect to MCUs that are geographically near them, reducing network traffic between sites to a single link to each MCU.

The RealPresence DMA system uses site topology information to cascade conferences for bandwidth. If you have a Polycom RealPresence Resource Manager system in your network, you can integrate your RealPresence DMA system with the RealPresence Resource Manager system to obtain its site topology data. You can then enable cascaded-for-bandwidth conferences with the following steps:

● On the Polycom RealPresence Resource Manager system, create site topology data defining the territories, sites, site links, and MPLS clouds in your network, and the subnets in each site.

● On the Polycom RealPresence DMA system, integrate with the Polycom RealPresence Resource Manager system to obtain its site topology data.

● On the Polycom RealPresence DMA system, enable cascading for bandwidth in some or all of your conference templates.

If you do not have a RealPresence Resource Manager system, you must define your site topology in the RealPresence DMA system instead of importing it.

Processing a Cascaded-for-Bandwidth Call

Once a conference with cascading for bandwidth enabled has started, the Polycom RealPresence DMA system uses the site topology information to route callers to the nearest eligible MCU (using the pool order applicable to the conference) that has available capacity:

● If the caller is in a site that contains one or more MCUs, the system selects an MCU in that site (it selects the same MCU that it would have chosen in the absence of cascading).

● If the caller is in a site that doesn’t contain MCUs, the system looks for MCUs in sites that only have a direct network path to the caller’s site (not through a cloud) and selects one.

● If there are no MCUs in sites that only have a direct network path to the caller’s site, the system looks for MCUs in sites that are connected to the caller’s site through a cloud and selects one.

● If an MCU belongs to an MCU pool, the DMA system selects an MCU that meets the requirements of the selection process from the highest priority pool within the pool order.

If a selected MCU is new to the conference, the RealPresence DMA system creates the cascade link to the hub MCU hosting the conference. The cascade link bandwidth matches the conference setting.

Cascaded conferences can have conference passcodes and can be Polycom Conferencing for Outlook (calendared) conferences.

Cascading for Size

Cascading for size makes it possible for a conference to contain many more participants than any single MCU could support and differs from cascading for bandwidth in two primary ways:

● Cascading for size does not use site topology information to choose additional MCUs for a conference.
Cascading for size supports a second level of cascade links so that a cascaded MCU can be either one link away from the "hub" MCU hosting the conference (this is a "spoke" MCU) or two links away (a "leaf" MCU linked to a "spoke").

To host a cascade-for-size conference, the RealPresence DMA system chooses the same MCU that it would have chosen in the absence of cascading except that for each existing cascade-for-size conference on an MCU, it subtracts the number of video ports reserved for cascading from the number of video ports available when calculating port availability.

Cascading for size may not be appropriate for all conferences and should be used selectively. In addition to possible transmission delays, each cascade-for-size conference reserves ports on the MCU, reducing the ports available for participants. Enabling cascading for size for conferences that do not require cascading underutilizes MCU resources.

**Note:** When a conference is cascaded across multiple MCUs, the video and audio from each MCU is transmitted to every other MCU through cascade links. This incurs some delay. In a conference with many cascade links, this delay may become noticeable to the participants. The transmission delay isn't noticeable in one-way communication or when all the speakers are on the same MCU. For this reason, large cascaded conferences are best suited to presentation-style conferences where only a few participants (on the same MCU) speak and the other participants only listen.

You can enable cascade-for-size conferences with these steps:

- Enable cascading for size in some or all of your conference templates.
- For one or more of your MCUs, specify the number of ports per cascade-for-size conference to reserve for cascade links.

**Processing a Cascaded-for-Size Call**

Once a conference with cascading for size enabled has started (the "hub" MCU has been chosen), the Polycom RealPresence DMA system completes the following process for each subsequent participant that dials into that conference:

- From among the MCUs that are currently part of the conference and have ports available that are not reserved for cascading, the RealPresence DMA system randomly selects one of the MCUs closest to the hub MCU, or the hub MCU itself.
- If on every MCU that is currently part of the conference, all available ports are reserved for cascading, the RealPresence DMA system does the following:
  - From among the MCUs that are currently part of the conference and that have ports available for the cascade link, the RealPresence DMA system selects the one closest to the hub MCU, or the hub MCU itself.
  - It selects a new MCU to join the conference, using the same selection process used for selecting the first (hub) MCU, and creates the cascade link to it.
  - If no MCU has ports available for cascade links, the RealPresence DMA system rejects the call.

**WebRTC Conferencing**

WebRTC participants start or enter a conference by connecting to the Polycom® RealPresence® Web Suite Experience Portal, which manages signaling between WebRTC clients and the RealPresence DMA system. The RealPresence DMA system cannot accept WebRTC calls directly from a WebRTC client.
Small conferences including up to three WebRTC participants do not require an MCU. This is known as “mesh” conferencing mode. In this mode, the WebRTC media streams are passed directly from client to client.

In certain conferencing situations, a mesh conference must be escalated to an MCU. When required, the RealPresence DMA system assigns a WebRTC-capable MCU to host the conference:

- If a fourth participant joins the conference
- If a non-WebRTC participant joins the conference
- If certain conference features are needed, such as conference recording

Once an MCU is assigned to host the conference, participants using WebRTC clients have the same experience as participants using SIP or H.323 endpoints. If a WebRTC client dials a conference that requires an MCU and the system selects an MCU that does not support WebRTC, the client is disconnected. For this reason, Polycom recommends creating MCU pool orders that consist only of MCUs that support WebRTC.

**WebRTC Conference Templates**

You can configure how the RealPresence DMA system handles conferences involving WebRTC participants by editing the conference template used for the conference.

The following limitations apply to WebRTC conferencing:

- WebRTC participants cannot enter conferences by dialing VEQs.
- WebRTC conferences do not support the **SVC only** conference mode.
- Some conference template settings are not compatible with the **WebRTC with mesh only** or **WebRTC with MCUs or mesh** settings.
- **WebRTC with mesh only** conference templates are not supported for Polycom® RealConnect™ conferences.
- Cisco Codian options are disabled when you enable WebRTC conferencing.

Some conference template settings are incompatible with mesh-only conferences. If you enable **WebRTC with mesh only** in a conference template and select incompatible settings, the system displays an error about the incompatibilities when you click OK in the **Add Conference Template** window. You can use this information to disable the incompatible features, or close the conference template dialog and begin again.

If a conference uses a template with the **WebRTC with MCUs or mesh** setting enabled, requesting a conference feature that is incompatible with mesh mode during a conference causes the system to promote the conference to an MCU. This allows the participant to use the requested feature, and the conference proceeds normally.

The following conference template settings are compatible with conferences in mesh mode. If you enable settings not in this list for a mesh-only conference, the RealPresence DMA system will display an error.

- **Polycom MCU General Settings**
  - Line rate
  - Encryption
  - Enable FECC
  - FW NAT keep alive
  - FW NAT keep alive interval (seconds)
● Polycom MCU Video Quality
   Multiple content resolutions

● Polycom MCU Video Settings
   Lecturer view switching

● Polycom MCU Audio Settings
   Mute participants except lecturer
   NoiseBlock™ (MPMx or newer)
   Speaker change threshold (MPMx or newer)

● Polycom MCU Site Names (all settings)

View the Conference Templates List

You can view the conference templates list for priority and descriptive information about each conference template.

The Polycom RealPresence DMA system comes with a Factory Template that has a default set of conference parameters. You can edit that template and create additional templates.

To view the conference templates list:

  » Go to Service Config > Conference Manager Setting > Conference Templates.

  The following table describes the fields in the Conference Templates list.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>The priority ranking of the template.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the template.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the template.</td>
</tr>
</tbody>
</table>

Add a Conference Template

You can add a standalone conference template and specify conference properties directly in the template. The Common Settings section applies to all MCUs. The Cisco Codian settings apply only if a Codian MCU is selected for a conference. The other sections apply only if a Polycom MCU is selected for a conference.

When the RealPresence DMA system uses a standalone template for a conference, the system sends the specific properties to the MCU instead of pointing to one of the MCU’s conference profiles.

To add a conference template:

  1  Go to Service Config > Conference Manager Settings > Conference Templates.

  2  Under Actions, click Add.
Specify the conference template settings based on the field descriptions in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Common Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>The name of the template (up to 50 characters).</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the conference template (up to 50 characters).</td>
</tr>
<tr>
<td>WebRTC</td>
<td>One of the following:</td>
</tr>
<tr>
<td></td>
<td>- <em>No WebRTC</em> — This template excludes WebRTC capability. WebRTC participants are disconnected upon attempting to connect to conferences using this conference template.</td>
</tr>
<tr>
<td></td>
<td>- <em>WebRTC with MCUs only</em> — Conferences using this template accept WebRTC, SIP, and H.323 participants, and the system promotes these conferences to a WebRTC-capable MCU as soon as the first participant connects.</td>
</tr>
<tr>
<td></td>
<td>- <em>WebRTC with mesh only</em> — Conferences using this template accept only WebRTC participants. All non-WebRTC participants are disconnected. Mesh only conferences allow up to three participants; if a fourth participant attempts to join, the new participant is disconnected.</td>
</tr>
<tr>
<td></td>
<td>- <em>WebRTC with MCUs or mesh</em> — Conferences using this template accept WebRTC participants. A WebRTC-only conference of up to three participants runs in mesh mode; if a fourth participant or non-WebRTC participant joins, the conference is automatically promoted to a WebRTC-capable MCU.</td>
</tr>
<tr>
<td><strong>Polycom MCU General Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Polycom MCU Profile Settings</td>
<td>See <a href="#">Two Types of Templates</a>.</td>
</tr>
<tr>
<td>Use existing profile</td>
<td>This option is only available when the WebRTC option <em>No WebRTC</em> is selected. Links this template to the Polycom MCU conference profile selected in the list below. Polycom recommends leaving this box unchecked and specifying conference properties directly.</td>
</tr>
<tr>
<td>Polycom MCU profile name</td>
<td>Identifies the profile to which this template is linked. The list contains the names of all the profiles available on the currently connected MCUs. If a profile is only available on some of the connected MCUs, its entry shows how many of the MCUs have that profile (for instance, 2 of 3). The system will put conferences using this template on the least used MCU that has this profile. If there are none, it selects the least-used MCU and either uses the Codian-specific settings (if it selected a Cisco Codian MCU) or falls back to the default conference template (if it selected a Polycom MCU).</td>
</tr>
</tbody>
</table>
Conference Templates

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conference Settings</td>
<td>One of the following:</td>
</tr>
<tr>
<td>Conference mode</td>
<td>• AVC only — Standard video conferencing mode supporting the H.264 Advanced Video Coding (AVC) compression standard. In an AVC conference, the MCU transcodes the video stream to each device in the conference to provide an optimal experience, based on its capabilities. This is the only mode that supports the use of Polycom MCU conference profiles, third-party and legacy endpoints, and Codian and legacy RMX MCUs.</td>
</tr>
<tr>
<td></td>
<td>• SVC only — video conferencing mode supporting the Annex G extension of the H.264 standard, known as H.264 Scalable Video Coding (SVC). An SVC video stream consists of a base layer stream that encodes the lowest available quality representation plus optional enhancement layer streams that each provide an additional quality improvement. The MCU passes the video streams from each device to each device. The number of enhancement layer streams sent to a device can be tailored to fit the bandwidth available and device capabilities. SVC conferencing is only possible with Polycom MCUs and endpoints that support H.264 SVC. Selecting this setting disables most of the other template settings.</td>
</tr>
<tr>
<td></td>
<td>• Mixed AVC and SVC — Enables both AVC-only endpoints and endpoints supporting SVC to join the conference. If the selected MCU doesn’t support SVC, the conference is started in AVC mode.</td>
</tr>
<tr>
<td>Conference mode experience</td>
<td>For mixed conference mode, specifies the video experience optimization strategy the MCU should implement. The experience optimization strategy determines the quality of the video streams that SVC participants receive from AVC participants. See the documentation for your Polycom MCU for detailed data regarding the resolutions each experience setting supports for various ranges of line rate. Note: All AVC callers must be capable of sending at a line rate available for the experience setting. SVC participants receive the same stream quality from all AVC endpoints, regardless of their individual capabilities.</td>
</tr>
<tr>
<td>Cascade for bandwidth</td>
<td>Enables conferences using this template to span Polycom MCUs to conserve network bandwidth. Cascading for bandwidth requires site topology information, which the Polycom RealPresence DMA system can get from a Polycom RealPresence Resource Manager system or you can create. This option and Cascade for size are mutually exclusive.</td>
</tr>
<tr>
<td>Cascade for size</td>
<td>Enables conferences using this template to span Polycom MCUs to achieve conference sizes larger than a single MCU can accommodate. This option and Cascade for bandwidth are mutually exclusive.</td>
</tr>
</tbody>
</table>

Polycom, Inc. 213
**Conference Templates**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Cascade for SVC             | When enabled, specifies that the cascade link between two Polycom MCUs will use SVC signaling. Can only be enabled when the conference mode is **Mixed AVC and SVC or SVC only**, and when **Cascade for bandwidth** or **Cascade for size** is selected.  
  When enabled, the system will select conference MCUs that are configured for SVC cascading, regardless of their position in the conference's pool order and even if MCUs with more capacity are available. If there are no MCUs available that are configured for SVC cascading, the following conditions apply:  
  • If **Cascade for size** is selected, the conference will start on an MCU but will not cascade.  
  • If **Cascade for bandwidth** is selected, the conference will not start.  
  When enabled with **Cascade for size**, a conference is limited to a hub and leaves configuration; three level cascading (with a hub, spokes, and leaves) is not supported. |
| Video switching (VSW)       | Enables a special conferencing mode that provides HD video while using MCU resources more efficiently. All participants see the current speaker full screen (the current speaker sees the previous speaker).  
  If this mode is enabled:  
  • The minimum line rate available is 768 kbps (except for SD resolution, available only on version 7 and newer Polycom MCUs with MPM+ or MPMx cards).  
  • All endpoints must connect at the same line rate, and those that don’t support the specified line rate are connected in voice-only mode.  
  • The video clarity, layout, and skins settings are not available.  
  • LPR is automatically turned off, but can be turned back on.  
  If this option is off, conferences using this template are in Continuous Presence (CP) mode, in which the MCU selects the best video protocol, resolution, and frame rate for each endpoint according to its capabilities. |
| H.264 high profile         | Sets a VSW conference to use Polycom's bandwidth-conserving H.264 High Profile codec (previously supported only in continuous presence mode).  
  If this is selected, all endpoints in the conference must support High Profile. Endpoints not connecting at the conference's exact line rate and resolution are connected in audio-only mode. Available only on version 7.6 and newer Polycom MCUs with MPMx cards. |
| Resolution                  | Available only if **Video switching** is selected. Offers various resolution settings, some of which are only available on Polycom MCUs with MPM+, MPMx, or MPMRx cards. |
| Line rate                   | The maximum bit rate at which endpoints can connect to conferences using this template.  
  If **Video switching** is selected, the minimum line rate is 768 kbps (except for SD resolution, available only on version 7 and newer Polycom MCUs with MPM+ or MPMx cards). |

**Advanced Settings**
## Field

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>Specifies the media encryption setting for conferences using this template:</td>
</tr>
<tr>
<td></td>
<td>• No encryption — All endpoints join unencrypted</td>
</tr>
<tr>
<td></td>
<td>• Encrypt when possible — Endpoints supporting encryption join encrypted; others join unencrypted.</td>
</tr>
<tr>
<td></td>
<td>• Encrypt all — Endpoints supporting encryption join encrypted; others cannot join.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> VMR dial-outs to H.323 endpoints from an encrypted RealPresence DMA system conference are unsupported and will not connect. Consult the MCU’s Administrator’s Guide for information about media encryption (SRTP).</td>
</tr>
<tr>
<td>Packet loss compensation</td>
<td>Enables Lost Packet Recovery (LPR) and Dynamic Bandwidth Allocation (DBA) for conferences using this template. LPR creates additional packets containing recovery information that can be used to reconstruct packets lost during transmission. DBA allocates the bandwidth needed to transmit the additional packets.</td>
</tr>
<tr>
<td>Exclusive content mode</td>
<td>When checked, if a participant is broadcasting content, prevent other participants from interrupting with their own content while the current content stream is active.</td>
</tr>
<tr>
<td>Enable FECC</td>
<td>When checked, enable Far End Camera Control for conference participants.</td>
</tr>
<tr>
<td>FW NAT keep alive</td>
<td>Specifies that when receiving calls through an SBC, the MCU should send media stream keep-alive messages to the SBC at the interval specified.</td>
</tr>
<tr>
<td>Interval (seconds)</td>
<td>Specifies how often to send keep-alive messages.</td>
</tr>
<tr>
<td>TIP compatibility</td>
<td>Enables compatibility with Cisco’s Telepresence Interoperability Protocol, either for video only or for both video and content. Conferences can include both endpoints that do not support TIP and Cisco TelePresence® System (CTS) endpoints. If Prefer TIP is selected, TIP content is used for endpoints that support TIP, and non-TIP content is used with non-TIP endpoints. Requires minimum line rate of 1024 kbps and HD resolution (720 or better). Available only on v7.6 and newer Polycom MCUs.</td>
</tr>
<tr>
<td>MS AVMCU cascade mode</td>
<td>When integrated with a Microsoft Skype for Business environment, controls behavior of the cascade link with the Skype for Business AVMCU.</td>
</tr>
<tr>
<td></td>
<td>• Resource Optimized — The cascade link between the RealPresence DMA system and the Skype for Business server’s AVMCU is limited to SD video resolutions to conserve MCU resources.</td>
</tr>
<tr>
<td></td>
<td>• Video Optimized — The cascade link between the RealPresence DMA system and the Skype for Business server’s AVMCU is capable of HD video resolutions, increasing MCU resource usage.</td>
</tr>
<tr>
<td>Enable MS panoramic layout</td>
<td>When integrated with a Microsoft environment (Lync 2013, Skype for Business 2015, or Office 365), enables a Polycom MCU to stream a panoramic layout from telepresence rooms or multiple non-Microsoft participants to Microsoft clients.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This option applies to on-premise and service provider deployment models.</td>
</tr>
</tbody>
</table>
### Field Templates

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Font for text over video** (MPMx or newer) | Allows you to specify the font type for text displayed to participants in a conference. If using **Default**, the system will display Heiti if a Chinese language is configured.  
**Note:** This property only applies when the MCU is configured for multilingual operation with Chinese (Simplified or Traditional) selected. |

### Polycom MCU Gathering Settings

| Enable gathering | Enables the gathering phase for conferences using this template. Not available if **Video switching** is selected.  
The gathering phase is a time period (configurable on the MCU) at the beginning of a conference when people are connecting. During this time, a slide is displayed that contains conference information, including a list of participants and some information you can specify here. |
| Displayed language | Language in which the gathering page is displayed. |
| Access number 1 | Optional access numbers to display on the gathering phase slide. |
| Access number 2 |  |
| Info1, Info2, Info3 | Optional free-form text fields to display on the gathering phase slide. Refer to the MCU's Administrator's Guide to see an example of the slide and the location and appearance of these fields.  
On a 16:9 endpoint, a maximum of 96 characters can be displayed for each field, and fewer on a 4:3 endpoint. |

### Polycom MCU Video Quality

| People Video Definition |  |
| Video quality | Offers two video optimizations:  
• Motion — higher frame rate  
• Sharpness — higher resolution  
Not available if **Conference mode** is set to **SVC only**. |
| Max resolution | Enables you to choose a resolution setting that limits the conference to no more than that resolution regardless of the line rate and resolution capabilities of the MCU and endpoints.  
Auto (the default) imposes no limit.  
Available only on version 7 and newer Polycom MCUs.  
Not available if **Conference mode** is set to **SVC only**. |
| Video clarity (MPM+ or newer) | Enables a video enhancement process that improves clarity, edge sharpness, and contrast on streams with resolutions up to and including SD.  
Available only on Polycom MCUs with MPM+ or MPMx cards. Not available if **Video switching** is selected.  
Not available if **Conference mode** is set to **SVC only**. |
| Auto brightness | Enables automatic balancing of brightness levels to compensate for an endpoint sending a dim image.  
Available only on v7 and newer Polycom MCUs.  
Not available if **Conference mode** is set to **SVC only**. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Content Video Definition</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Content settings</strong></td>
<td>The transmission mode for the Content channel:</td>
</tr>
<tr>
<td></td>
<td>• Graphics — lowest bit rate for basic graphics</td>
</tr>
<tr>
<td></td>
<td>• High-resolution graphics — higher bit rate for better graphics resolution</td>
</tr>
<tr>
<td></td>
<td>• Live video — the Content channel is used for live video</td>
</tr>
<tr>
<td></td>
<td>• Customized content rate — allows you to specify a Content rate</td>
</tr>
<tr>
<td></td>
<td>A higher bit rate for the Content channel reduces the bit rate for the People channel.</td>
</tr>
<tr>
<td><strong>Content rate</strong></td>
<td>Bit rate of the content channel. Enabled when the Customized content rate content setting is selected.</td>
</tr>
<tr>
<td><strong>AS SIP content</strong></td>
<td>Enables the sharing of content using the AS-SIP protocol security features.</td>
</tr>
<tr>
<td><strong>Multiple content resolutions</strong></td>
<td>Enables content sharing over multiple video streams. When selected, you can choose which protocols to use for each stream with the Transcode to setting.</td>
</tr>
<tr>
<td></td>
<td><em>Note:</em> Enabled only when:</td>
</tr>
<tr>
<td></td>
<td>- Conference mode is set to AVC only.</td>
</tr>
<tr>
<td></td>
<td>- TIP compatibility is set to either None or Video Only.</td>
</tr>
<tr>
<td><strong>Transcode to</strong></td>
<td>Enables you to choose which protocols to use for each stream of content. Enabled when the Multiple content resolutions check box is selected.</td>
</tr>
<tr>
<td></td>
<td><em>Note:</em> The H.264 protocol check box is always selected.</td>
</tr>
<tr>
<td><strong>Content protocol</strong></td>
<td>Content channel protocol options:</td>
</tr>
<tr>
<td></td>
<td>• Use H.263.</td>
</tr>
<tr>
<td></td>
<td>• Use H.264 if available, otherwise use H.263.</td>
</tr>
<tr>
<td></td>
<td>• Use H.264 cascade and SVC optimized.</td>
</tr>
<tr>
<td></td>
<td>• Use H.264 HD.</td>
</tr>
<tr>
<td><strong>Content resolution</strong></td>
<td>Specifies the resolution of the content channel for the conference and cascade link.</td>
</tr>
<tr>
<td></td>
<td>Available only when Content protocol is set to H.264 cascade and SVC optimized.</td>
</tr>
<tr>
<td><strong>H.264 high profile</strong></td>
<td>Enables the H.264 High Profile set of capabilities for the content channel, which enables additional compression efficiency and allows for higher resolutions to use the same bandwidth.</td>
</tr>
<tr>
<td><strong>Send content to legacy endpoints (MPM+ or newer)</strong></td>
<td>Enables endpoints that don’t support H.239 to receive the Content channel over the video (People) channel.</td>
</tr>
</tbody>
</table>
Enable MS RDP content

When selected, the RealPresence DMA system starts conferences based on this template only on Modular MCUs (MMCU) that have sufficient soft blade resources. MMCUs may be configured with an RDP translator that converts H.264 content shared from a standard endpoint to RDP content to deliver to a Skype ASMCU. Likewise, when a Skype client shares RDP content, the RDP translator delivers H.264 content to the MMCU.

If not selected, the system considers all MCUs within the MCU pool order when starting a conference. However, even if the system selects an MMCU configured with an RDP translator, RDP content will not be delivered to or from Skype clients.

If an MCU failover occurs, video is automatically reconnected, but content is not re-established. The Skype conference or client must re-initiate content.

Note: This option can be used in place of a separate Polycom® ContentConnect™ gateway solution.

Polycom MCU Video Settings

Presentation mode Enables a conference to change to lecture mode when the current speaker speaks for 30 seconds. When another participant starts talking, it returns to the previous video layout.

Not available if Video switching or Same layout is selected, or if Telepresence mode is Yes.

Same layout Forces the selected layout on all participants. Personal selection of the video layout is disabled.

Not available if Presentation mode or Video switching is selected, or if Telepresence mode is Yes.

Lecturer view switching When in lecture mode, enables the lecturer’s view to automatically switch among participants (if the number exceeds the number of windows in the layout) while the lecturer is talking.

Not available if Same layout is selected or Telepresence mode is Yes.

Auto layout Lets the system select the video layout based on the number of participants in conference. Clear the check box to select a specific layout (below).

Not available if Video switching is selected or Telepresence mode is Yes.

Layout With Auto layout unchecked, you can select the number and arrangement of video frames. Once you choose a layout, a small representation of it displays here.

Not available if Video switching is selected.

Telepresence mode Support for telepresence conference rooms joining the conference:

- Auto (default) – A conference is automatically put into telepresence mode when a telepresence endpoint (RPX, TPX, ATX, or OTX) joins. Recommended setting.
- On – Telepresence mode is on, regardless of whether a telepresence endpoint is present.
- Off – Telepresence mode is off, regardless of whether a telepresence endpoint is present.

Note: The system flag ITP_CERTIFICATION must be set to YES. See the information about system flags in the MCU’s Administrator’s Guide.
Polycom, Inc. 219

Telepresence layout mode

- Manual – Layout is controlled manually by a conference operator using the Multipoint Layout Application (MLA) interface.
- Continuous Presence – Tells the MLA to generate a multipoint view (standard or custom).
- Room Switch – Tells the MLA to use Voice Activated Room Switching (VARS). The speaker’s site is the only one seen by others.
- Speaker Priority – Ensures that the current speaker is always displayed in the video layout. The previous speakers are also displayed if there is room in the layout. In this mode, each endpoint in the conference reserves screens for displaying the active speaker in the largest video layout cell available.
- Participants Priority – Uses a dynamic video layout that includes as many participants as possible.

Not available if Telepresence mode is No. See the Polycom Multipoint Layout Application User Guide for more information about layouts.

Polycom MCU Audio Settings

- Echo suppression
  Enables the MCU to detect and suppress echo. Available only on MCUs with MPM+ or MPMx cards.

- Keyboard noise suppression
  Enables the MCU to detect and suppress keyboard noise. Available only on MCUs with MPM+ or MPMx cards.

- Audio clarity
  Improves the voice quality in conference of a PSTN endpoint. Available only on version 7 and newer Polycom MCUs.

- Mute participants except lecturer
  Enables the MCU to automatically mute all participants except the lecturer upon connection to the conference.

- NoiseBlock™ (MPMx or newer)
  Enables the MCU to automatically detect and mute endpoints that have a noisy audio channel. Not available on MCUs with an MPM+ card.

- Speaker change threshold (seconds) (MPMx or newer)
  Allows you to configure the amount of time the MCU requires a participant to speak continuously until becoming the speaker. The default Auto setting is 3 seconds.

Polycom MCU Skins

Enables you to choose the display appearance (skin) for conferences using this template. Not available if Telepresence mode is Yes or Video switching is enabled.
### Polycom MCU Conference IVR

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Override default conference IVR service</strong></td>
<td>Links this template to the specific conference IVR service selected in the list below. <strong>Note:</strong> The Polycom MCU conference IVR service is separate and distinct from the RealPresence DMA system’s SIP-only shared number dialing feature (see Shared Number Dialing). For most purposes, this option should not be selected. That enables the system to choose one of two defaults, depending on whether callers need to be prompted for passcodes. If you do select this option, be sure the IVR service you select is appropriate for the users who will use this template. See your Polycom MCU documentation for information about conference IVR services.</td>
</tr>
<tr>
<td><strong>Conference IVR service</strong></td>
<td>The list contains the names of all the conference IVR services available on the currently connected MCUs. If an IVR service is only available on some of the connected MCUs, its entry shows how many of the MCUs have that IVR service (for instance, 2 of 3). The system will put conferences using this template on the least used MCU that has the selected conference IVR service. If there are none, it falls back to the default conference IVR service.</td>
</tr>
<tr>
<td><strong>Conference requires chairperson</strong></td>
<td>Conferences based on this template don’t start until a chairperson joins (callers arriving earlier are placed on hold) and may end when the last chairperson leaves (depending on the MCU configuration). This option is ignored if the user doesn’t have a chairperson passcode. For enterprise users, chairperson passcodes can come from the Active Directory, but you can override the Active Directory value. For local users, you can add or change chairperson passcodes when you create or edit the users. <strong>Note:</strong> If this option is enabled and this template is used for a Polycom RealConnect™ conference, the Skype for Business presenter acts as the chairperson for that conference.</td>
</tr>
<tr>
<td><strong>Terminate conference after chairperson drops</strong></td>
<td>If this template is used for a conference with a chairperson passcode, the conference is terminated when the chairperson leaves the conference. A message is played to the remaining participants informing them that the chairperson has left the conference.</td>
</tr>
</tbody>
</table>

### Polycom MCU Site Names

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Display mode** | Overlays the endpoint display name on each video participant’s display in a Continuous Presence conference:  
  • Auto – Display site names only when the layout changes.  
  • On – Always display site names.  
  • Off – Do not display site names (default). |
| **Font size** | Controls the font size for the site name text. The default value is 12. |
| **Color** | Allows you to configure the site name font appearance. When you select one of the Polycom MCU Skins with a background image, there are more color choices available for selection. |
**Conference Templates**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display position</td>
<td>Controls the position of the text within the video participant's display with preset or custom locations. The value changes to Custom if you use the Horizontal position or Vertical position sliders to change the position to one that is not defined by a preset value.</td>
</tr>
<tr>
<td>Horizontal position</td>
<td>Allows you to manually control the horizontal position of the site name text.</td>
</tr>
<tr>
<td>Vertical position</td>
<td>Allows you to manually control the vertical position of the site name text.</td>
</tr>
<tr>
<td>Background transparency</td>
<td>When you choose one of the Polycom MCU Skins with a background image, you can use this slider to control the transparency of the site name font background.</td>
</tr>
</tbody>
</table>

**Polycom MCU Recording**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Record conference          | The conference recording setting for this template:  
• Disabled – Recording isn’t available for conferences using this template.  
• Immediately – Recording starts automatically when the conference starts.  
• Upon Request – Recording can be initiated manually by the chairperson or an operator. Conference recording requires a Polycom RealPresence Media Suite or Polycom Capture Server recording system and an MCU that supports recording. |
| Dial out recording link    | Select a specific recording link or the MCU’s default. The list contains the names of all recording links available on the connected MCUs, with the number of MCUs that have the link shown in parentheses. Available only on version 7 and newer Polycom MCUs. |
| Audio only                 | Limits recording to the audio channel of the conference.                                                                                      |
| Indication of recording    | Displays a red dot recording indicator in the upper left corner of the video layout. Available only on version 7.1 and newer Polycom MCUs.         |
| Play recording message (V8.4 or newer) | Available with version 8.4 or newer RealPresence Collaboration Server MCUs.                                                                  |

**Polycom MCU Indications**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Position</td>
<td>Use the drop-down menu to set the display position of the indication icons group.</td>
</tr>
<tr>
<td>Recordings</td>
<td>Enables the Recording icon, which is displayed if a recording is in progress.</td>
</tr>
<tr>
<td>Media type indications</td>
<td></td>
</tr>
<tr>
<td>Audio participants</td>
<td>Select the check box to enable the Audio Participants icon.</td>
</tr>
<tr>
<td>Video participants</td>
<td>Select the check box to enable the Video Participants icon.</td>
</tr>
<tr>
<td>Display mode</td>
<td>Select a radio button to change when and for how long the MCU displays the Audio Participants and Video Participants icons.</td>
</tr>
</tbody>
</table>
### Permanent
The MCU displays the icon permanently when audio or video participants are connected.

### On participant join or leave
The MCU displays the icon only for a short time when the number of audio or video participants changes.

### Duration
Allows you to select the length of time the icon is visible upon a participant joining or leaving.

### Network Quality
Enables the MCU to display the Network Quality icon, which indicates the network quality for any individuals experiencing significant packet loss.

### Polycom MCU Message Overlay

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>Enables or disables Message Overlay (disabled by default).</td>
</tr>
<tr>
<td>Content</td>
<td>Enter the message text. The message text can be up to 50 Unicode characters.</td>
</tr>
<tr>
<td>Font size</td>
<td>Click the arrows to adjust the font size of the message text. The default is 24 points. Note: In some languages, when a large font size is selected, both rolling and static messages may be truncated if the message length exceeds the resolution width.</td>
</tr>
<tr>
<td>Color</td>
<td>Select the color and background of the message text. The default is white text on a red background.</td>
</tr>
<tr>
<td>Vertical position</td>
<td>Move the slider to the right to move the vertical position of the displayed text downward within the Video Layout. Move the slider to the left to move the vertical position of the displayed text upward within the Video Layout.</td>
</tr>
<tr>
<td>Background transparency</td>
<td>Move the slider to the left to decrease the transparency of the background of the message text. A transparency of 0 indicates no transparency (solid background color). Move the slider to the right to increase the transparency of the background of the message text. A transparency of 100 indicates full transparency (no background color). The default is 50.</td>
</tr>
<tr>
<td>Display repetition</td>
<td>Click the arrows to increase or decrease the number of times that the text message display is to be repeated. The default is 3.</td>
</tr>
<tr>
<td>Display speed</td>
<td>Select whether the message is static or moves across the screen. If moving, choose the movement speed. The default speed is Slow.</td>
</tr>
</tbody>
</table>
### Cisco Codian

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Floor and chair control      | Specifies how much control conference participants may have:  
  - Do not allow floor or chair control – Participants have no control.  
  - Allow floor control only – A participant may “take the floor.” Everyone sees that participant’s video full-screen.  
  - Allow floor and chair control – A participant may also “take the chair.” The chair can designate whose video everyone sees full-screen. The chair can also disconnect participants.  
  This setting works only in H.323 conferences and only if H.243 Floor and Chair Control is enabled on the MCU. All endpoints must support H.243 chair control. |
| Automatic lecture mode (4.1) | Enables the MCU to put a conference into lecture mode, either immediately or after the speaker has been talking for the selected interval. In lecture mode, the lecturer (speaker) is displayed full-screen to the other participants. The lecturer sees the normal continuous presence view.  
  Available only on Codian v4.1 MCUs. |
| Layout control via FECC/DTMF  | Enables participants to change their individual layouts using far end camera control, with or without fallback to touchtone commands for endpoints that don’t support FECC.  
  FECC without fallback is available only on Codian v4.1 MCUs. |
| Mute in-band DTMF (4.1)      | Specifies whether the MCU mutes participants’ in-band DTMF (touchtones) so that other participants don’t hear them:  
  - When used for MCU control  
  - Always  
  - Never  
  Available only on Codian version 4.1 MCUs. |
| Allow DTMF *6 to mute audio  | Enables conference participants to mute themselves using the *6 touchtone command.  
  Available only on Codian version 4.1 MCUs. |
| (4.1)                        |                                                                                                                                                                                                          |
| Content channel video        | Enables the conference to support a second video stream for content. This setting works only if Content Status is enabled on the MCU.                                                                     |
| Transmitted content resolutions (4.1) | Specifies the aspect ratio used for the content channel. If Allow all resolutions is selected, endpoints with a 16:9 aspect ratio receive that, and others receive 4:3.  
  Available only on Codian version 4.1 MCUs. |
| Conference custom layout     | Enables the Conference layout desired setting, where you can select the number and arrangement of video frames by clicking the image.                                                                     |
| Conference layout desired    | With Conference custom layout enabled, allows you to select the number and arrangement of video frames by clicking the image. Once a layout is chosen, a small representation of it appears here. See Select a Video Frames Layout. |

4 Click OK.
Edit a Conference Template

You can edit a conference template when necessary. The **Common Settings** section applies to all MCUs. The **Cisco Codian** section appears only if the system is licensed to use Cisco Codian MCUs, and its settings apply only if a Codian MCU is selected for the call. The other sections apply only if a Polycom MCU is selected.

**To edit a conference template:**

1. Go to **Service Config > Conference Manager Setting > Conference Templates**.
2. In the **Conference Templates** list, select the template of interest and click **Edit**.

The following table describes the fields in the dialog.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Common Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>A meaningful name for the template (up to 50 characters).</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the conference template (up to 50 characters).</td>
</tr>
<tr>
<td>WebRTC</td>
<td>One of the following:</td>
</tr>
<tr>
<td></td>
<td>• <em>No WebRTC</em> — This template excludes WebRTC capability. WebRTC participants are disconnected upon attempting to connect to conferences using this conference template.</td>
</tr>
<tr>
<td></td>
<td>• <em>WebRTC with MCUs only</em> — Conferences using this template accept WebRTC, SIP, and H.323 participants, and the system promotes these conferences to a WebRTC-capable MCU as soon as the first participant connects.</td>
</tr>
<tr>
<td></td>
<td>• <em>WebRTC with mesh only</em> — Conferences using this template accept only WebRTC participants. Mesh only conferences allow up to three participants; if a fourth participant attempts to join, the new participant is disconnected.</td>
</tr>
<tr>
<td></td>
<td>• <em>WebRTC with MCUs or mesh</em> — Conferences using this template accept WebRTC participants. A WebRTC-only conference of up to three participants runs in mesh mode; if a fourth participant joins, the conference is automatically promoted to a WebRTC-capable MCU.</td>
</tr>
</tbody>
</table>

**Polycom MCU General Settings**

<table>
<thead>
<tr>
<th>Polycom MCU Profile Settings</th>
<th>See <a href="#">Two Types of Templates</a>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use existing profile</td>
<td>This option is only available when the WebRTC option <strong>No WebRTC</strong> is selected. Links this template to the Polycom MCU conference profile selected in the list below. Polycom recommends leaving this box unchecked and specifying conference properties directly.</td>
</tr>
</tbody>
</table>
## Polycom MCU profile name
Identifies the profile to which this template is linked. The list contains the names of all the profiles available on the currently connected MCUs. If a profile is only available on some of the connected MCUs, its entry shows how many of the MCUs have that profile (for instance, 2 of 3).

The system will put conferences using this template on the least used MCU that has this profile. If there are none, it selects the least-used MCU and either uses the Codian-specific settings (if it selected a Cisco Codian MCU) or falls back to the default conference template (if it selected a Polycom MCU).

## Conference Settings
### Conference mode
One of the following:

- **AVC only** — Standard video conferencing mode supporting the H.264 Advanced Video Coding (AVC) compression standard. In an AVC conference, the MCU transcodes the video stream to each device in the conference to provide an optimal experience, based on its capabilities.

  This is the only mode that supports the use of Polycom MCU conference profiles, third-party and legacy endpoints, and Codian and legacy RMX MCUs.

- **SVC only** — video conferencing mode supporting the Annex G extension of the H.264 standard, known as H.264 Scalable Video Coding (SVC). An SVC video stream consists of a base layer stream that encodes the lowest available quality representation plus optional enhancement layer streams that each provide an additional quality improvement. The MCU passes the video streams from each device to each device.

  The number of enhancement layer streams sent to a device can be tailored to fit the bandwidth available and device capabilities. SVC conferencing is only possible with Polycom MCUs and endpoints that support H.264 SVC. Selecting this setting disables most of the other template settings.

- **Mixed AVC and SVC** — Enables both AVC-only endpoints and endpoints supporting SVC to join the conference. If the selected MCU doesn’t support SVC, the conference is started in AVC mode.

  **Note:** If the MCU supports SVC but not mixed mode, the conference fails to start.

### Conference mode experience
For mixed conference mode, specifies the video experience optimization strategy the MCU should implement. The experience optimization strategy determines the quality of the video streams that SVC participants receive from AVC participants.

See the documentation for your Polycom MCU for detailed data regarding the resolutions each experience setting supports for various ranges of line rate.

**Note:** All AVC callers must be capable of sending at a line rate available for the experience setting. SVC participants receive the same stream quality from all AVC endpoints, regardless of their individual capabilities.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polycom MCU profile name</td>
<td>Identifies the profile to which this template is linked. The list contains the names of all the profiles available on the currently connected MCUs. If a profile is only available on some of the connected MCUs, its entry shows how many of the MCUs have that profile (for instance, 2 of 3). The system will put conferences using this template on the least used MCU that has this profile. If there are none, it selects the least-used MCU and either uses the Codian-specific settings (if it selected a Cisco Codian MCU) or falls back to the default conference template (if it selected a Polycom MCU).</td>
</tr>
<tr>
<td>Conference Settings</td>
<td></td>
</tr>
<tr>
<td>Conference mode</td>
<td>One of the following:</td>
</tr>
</tbody>
</table>
|                     | • **AVC only** — Standard video conferencing mode supporting the H.264 Advanced Video Coding (AVC) compression standard. In an AVC conference, the MCU transcodes the video stream to each device in the conference to provide an optimal experience, based on its capabilities.  
  This is the only mode that supports the use of Polycom MCU conference profiles, third-party and legacy endpoints, and Codian and legacy RMX MCUs. |
|                     | • **SVC only** — video conferencing mode supporting the Annex G extension of the H.264 standard, known as H.264 Scalable Video Coding (SVC). An SVC video stream consists of a base layer stream that encodes the lowest available quality representation plus optional enhancement layer streams that each provide an additional quality improvement. The MCU passes the video streams from each device to each device.  
  The number of enhancement layer streams sent to a device can be tailored to fit the bandwidth available and device capabilities. SVC conferencing is only possible with Polycom MCUs and endpoints that support H.264 SVC. Selecting this setting disables most of the other template settings. |
|                     | • **Mixed AVC and SVC** — Enables both AVC-only endpoints and endpoints supporting SVC to join the conference. If the selected MCU doesn’t support SVC, the conference is started in AVC mode.  
  **Note:** If the MCU supports SVC but not mixed mode, the conference fails to start. |
| Conference mode experience | For mixed conference mode, specifies the video experience optimization strategy the MCU should implement. The experience optimization strategy determines the quality of the video streams that SVC participants receive from AVC participants. See the documentation for your Polycom MCU for detailed data regarding the resolutions each experience setting supports for various ranges of line rate.  
 **Note:** All AVC callers must be capable of sending at a line rate available for the experience setting. SVC participants receive the same stream quality from all AVC endpoints, regardless of their individual capabilities. |
Conference Templates

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cascade for bandwidth</td>
<td>Enables conferences using this template to span Polycom MCUs to conserve network bandwidth. Cascading for bandwidth requires site topology information, which the Polycom RealPresence DMA system can get from a Polycom RealPresence Resource Manager system or you can create. This option and Cascade for size are mutually exclusive.</td>
</tr>
<tr>
<td>Cascade for size</td>
<td>Enables conferences using this template to span Polycom MCUs to achieve conference sizes larger than a single MCU can accommodate. This option and Cascade for bandwidth are mutually exclusive.</td>
</tr>
</tbody>
</table>
| Video switching (VSW)         | Enables a special conferencing mode that provides HD video while using MCU resources more efficiently. All participants see the current speaker full screen (the current speaker sees the previous speaker). If this mode is enabled:  
  • The minimum line rate available is 768 kbps (except for SD resolution, available only on version 7 and newer Polycom MCUs with MPM+ or MPMx cards).
  • All endpoints must connect at the same line rate, and those that don’t support the specified line rate are connected in voice-only mode.
  • The video clarity, layout, and skins settings are not available.
  • LPR is automatically turned off, but can be turned back on. If this option is off, conferences using this template are in Continuous Presence (CP) mode, in which the MCU selects the best video protocol, resolution, and frame rate for each endpoint according to its capabilities. |
| H.264 high profile           | Sets a VSW conference to use Polycom’s bandwidth-conserving H.264 High Profile codec (previously supported only in continuous presence mode). If this is selected, all endpoints in the conference must support High Profile. Endpoints not connecting at the conference’s exact line rate and resolution are connected in audio-only mode. Available only on version 7.6 and newer Polycom MCUs with MPMx cards. |
| Resolution                    | Available only if Video switching is selected. Offers various resolution settings, some of which are only available on Polycom MCUs with MPM+, MPMx, or MPMRx cards. |
| Line rate                     | The maximum bit rate at which endpoints can connect to conferences using this template. If Video switching is selected, the minimum line rate is 768 kbps (except for SD resolution, available only on version 7 and newer Polycom MCUs with MPM+ or MPMx cards). |

Advanced Settings
## Conference Templates

### Encryption

Specifies the media encryption setting for conferences using this template:
- **No encryption** — All endpoints join unencrypted.
- **Encrypt when possible** — Endpoints supporting encryption join encrypted; others join unencrypted.
- **Encrypt all** — Endpoints supporting encryption join encrypted; others can’t join.

**Note:** VMR dial-outs to H.323 endpoints from an encrypted RealPresence DMA system conference are unsupported and will not connect. Consult the MCU’s Administrator’s Guide for information about media encryption (SRTP).

### LPR

Enables Lost Packet Recovery for conferences using this template. LPR creates additional packets containing recovery information that can be used to reconstruct packets lost during transmission.

### TIP compatibility

Enables compatibility with Cisco’s Telepresence Interoperability Protocol, either for video only or for both video and content. Conferences can include both endpoints that don’t support TIP and Cisco TelePresence® System (CTS) endpoints. If Prefer TIP is selected, TIP content is used for endpoints that support TIP, and non-TIP content is used with non-TIP endpoints. Requires minimum line rate of 1024 kbps and HD resolution (720 or better). Available only on v7.6 and newer Polycom MCUs.

### MS AVMCU cascade mode

When integrated with a Microsoft Skype for Business environment, controls behavior of the cascade link with the Skype for Business AVMCU.
- **Resource Optimized** — The cascade link between the RealPresence DMA system and the Skype for Business server’s AVMCU is limited to SD video resolutions to conserve MCU resources.
- **Video Optimized** — The cascade link between the RealPresence DMA system and the Skype for Business server’s AVMCU is capable of HD video resolutions, increasing MCU resource usage.

### Enable MS panoramic layout

When integrated with a Microsoft environment (Lync 2013, Skype for Business 2015, or Office 365), enables a Polycom MCU to stream a panoramic layout from telepresence rooms or multiple non-Microsoft participants to Microsoft clients.

**Note:** This option applies to on-premise and service provider deployment models.

### FW NAT keep alive

Specifies that when receiving calls through an SBC, the MCU should send media stream keep-alive messages to the SBC at the interval specified.

### Interval (seconds)

Specifies how often to send keep-alive messages.

### Enable FECC

When checked, enable Far End Camera Control for conference participants.

### Exclusive content mode

When checked, if a participant is broadcasting content, prevent other participants from interrupting with their own content while the current content stream is active.

### Table

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>Specifies the media encryption setting for conferences using this template:</td>
</tr>
<tr>
<td></td>
<td>- <strong>No encryption</strong> — All endpoints join unencrypted.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Encrypt when possible</strong> — Endpoints supporting encryption join encrypted; others join unencrypted.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Encrypt all</strong> — Endpoints supporting encryption join encrypted; others can’t join.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> VMR dial-outs to H.323 endpoints from an encrypted RealPresence DMA system conference are unsupported and will not connect. Consult the MCU’s Administrator’s Guide for information about media encryption (SRTP).</td>
</tr>
<tr>
<td>LPR</td>
<td>Enables Lost Packet Recovery for conferences using this template. LPR creates additional packets containing recovery information that can be used to reconstruct packets lost during transmission.</td>
</tr>
<tr>
<td>TIP compatibility</td>
<td>Enables compatibility with Cisco’s Telepresence Interoperability Protocol, either for video only or for both video and content. Conferences can include both endpoints that don’t support TIP and Cisco TelePresence® System (CTS) endpoints. If Prefer TIP is selected, TIP content is used for endpoints that support TIP, and non-TIP content is used with non-TIP endpoints. Requires minimum line rate of 1024 kbps and HD resolution (720 or better). Available only on v7.6 and newer Polycom MCUs.</td>
</tr>
<tr>
<td>MS AVMCU cascade mode</td>
<td>When integrated with a Microsoft Skype for Business environment, controls behavior of the cascade link with the Skype for Business AVMCU.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Resource Optimized</strong> — The cascade link between the RealPresence DMA system and the Skype for Business server’s AVMCU is limited to SD video resolutions to conserve MCU resources.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Video Optimized</strong> — The cascade link between the RealPresence DMA system and the Skype for Business server’s AVMCU is capable of HD video resolutions, increasing MCU resource usage.</td>
</tr>
<tr>
<td>Enable MS panoramic layout</td>
<td>When integrated with a Microsoft environment (Lync 2013, Skype for Business 2015, or Office 365), enables a Polycom MCU to stream a panoramic layout from telepresence rooms or multiple non-Microsoft participants to Microsoft clients. Note: This option applies to on-premise and service provider deployment models.</td>
</tr>
<tr>
<td>FW NAT keep alive</td>
<td>Specifies that when receiving calls through an SBC, the MCU should send media stream keep-alive messages to the SBC at the interval specified.</td>
</tr>
<tr>
<td>Interval (seconds)</td>
<td>Specifies how often to send keep-alive messages.</td>
</tr>
<tr>
<td>Enable FECC</td>
<td>When checked, enable Far End Camera Control for conference participants.</td>
</tr>
<tr>
<td>Exclusive content mode</td>
<td>When checked, if a participant is broadcasting content, prevent other participants from interrupting with their own content while the current content stream is active.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>
| Font for text over video (MPMx or newer) | Allows you to specify the font type for text displayed to participants in a conference. If using **Default** the system will display Heiti if a Chinese language is configured.  
**Note:** This property only applies when the MCU is configured for multilingual operation with Chinese (Simplified or Traditional) selected. |

**Polycom MCU Gathering Settings**

| Enable gathering | Enables the gathering phase for conferences using this template. Not available if **Video switching** is selected.  
This is a time period (configurable on the MCU) at the beginning of a conference when people are connecting. During this time, a slide is displayed that contains conference information, including a list of participants and some information you can specify here. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Displayed language</td>
<td>Language in which the gathering page is displayed.</td>
</tr>
<tr>
<td>Access number 1</td>
<td>Optional access numbers to display on the gathering phase slide.</td>
</tr>
<tr>
<td>Access number 2</td>
<td></td>
</tr>
</tbody>
</table>
| Info1, Info2, Info3 | Optional free-form text fields to display on the gathering phase slide. Refer to the MCU's *Administrator's Guide* to see an example of the slide and the location and appearance of these fields.  
On a 16:9 endpoint, a maximum of 96 characters can be displayed for each field, and fewer on a 4:3 endpoint. |

**Polycom MCU Video Quality**

<table>
<thead>
<tr>
<th>People Video Definition</th>
<th></th>
</tr>
</thead>
</table>
| Video quality | Offers two video optimizations:  
- **Motion** — higher frame rate  
- **Sharpness** — higher resolution  
Not available if **Conference mode** is set to **SVC only**. |
| Max resolution | Enables you to choose a resolution setting that limits the conference to no more than that resolution regardless of the line rate and resolution capabilities of the MCU and endpoints.  
Auto (the default) imposes no limit.  
Available only on version 7 and newer Polycom MCUs.  
Not available if **Conference mode** is set to **SVC only**. |
| Video clarity (MPM+ or newer) | Enables a video enhancement process that improves clarity, edge sharpness, and contrast on streams with resolutions up to and including SD.  
Available only on Polycom MCUs with MPM+ or MPMx cards. Not available if **Video switching** is selected.  
Not available if **Conference mode** is set to **SVC only**. |
| Auto brightness | Enables automatic balancing of brightness levels to compensate for an endpoint sending a dim image.  
Available only on v7 and newer Polycom MCUs.  
Not available if **Conference mode** is set to **SVC only**. |
### Field Video Definition

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content settings</td>
<td>The transmission mode for the Content channel:</td>
</tr>
<tr>
<td></td>
<td>• Graphics — lowest bit rate for basic graphics</td>
</tr>
<tr>
<td></td>
<td>• High-resolution graphics — higher bit rate for better graphics resolution</td>
</tr>
<tr>
<td></td>
<td>• Live video — the Content channel is used for live video</td>
</tr>
<tr>
<td></td>
<td>• Customized content rate — allows you to specify a <strong>Content rate</strong> A higher bit rate for the Content channel reduces the bit rate for the People channel.</td>
</tr>
<tr>
<td>Content rate</td>
<td>Bit rate of the content channel. Enabled when the <strong>Customized content rate</strong> content setting is selected.</td>
</tr>
<tr>
<td>AS SIP content</td>
<td>Enables the sharing of content using the AS-SIP protocol security features.</td>
</tr>
<tr>
<td>Multiple content resolutions</td>
<td>Enables content sharing over multiple video streams. When selected, you can choose which protocols to use for each stream with the <strong>Transcode to</strong> setting.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Enabled only when:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Conference mode</strong> is set to <strong>AVC only</strong>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>TIP compatibility</strong> is set to either <strong>None</strong> or <strong>Video Only</strong>.</td>
</tr>
<tr>
<td>Transcode to</td>
<td>Enables you to choose which protocols to use for each stream of content. Enabled when the <strong>Multiple content resolutions</strong> check box is selected.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The <strong>H.264</strong> protocol check box is always selected.</td>
</tr>
<tr>
<td>Content protocol</td>
<td>Content channel protocol options:</td>
</tr>
<tr>
<td></td>
<td>• Use H.263.</td>
</tr>
<tr>
<td></td>
<td>• Use H.264 if available, otherwise use H.263.</td>
</tr>
<tr>
<td></td>
<td>• Use H.264 cascade and SVC optimized.</td>
</tr>
<tr>
<td></td>
<td>• Use H.264 HD.</td>
</tr>
<tr>
<td>Content resolution</td>
<td>Specifies the resolution of the content channel for the conference and cascade link.</td>
</tr>
<tr>
<td></td>
<td>Available only when <strong>Content protocol</strong> is set to <strong>H.264 cascade and SVC optimized</strong>.</td>
</tr>
<tr>
<td>H.264 high profile</td>
<td>Enables the H.264 High Profile set of capabilities for the content channel, which enables additional compression efficiency and allows for higher resolutions to use the same bandwidth.</td>
</tr>
<tr>
<td>Send content to legacy endpoints (MPM+ or newer)</td>
<td>Enables endpoints that don’t support H.239 to receive the Content channel over the video (People) channel.</td>
</tr>
<tr>
<td></td>
<td>Available only on MCUs with MPM+ and MPMx cards. Not available if <strong>Video switching</strong> or <strong>Same layout</strong> is selected, or if <strong>Telepresence mode</strong> is Yes.</td>
</tr>
</tbody>
</table>
When selected, the RealPresence DMA system starts conferences based on this template only on Modular MCUs (MMCU) that have sufficient soft blade resources. MMCUs may be configured with an RDP translator that converts H.264 content shared from a standard endpoint to RDP content to deliver to a Skype ASMCU. Likewise, when a Skype client shares RDP content, the RDP translator delivers H.264 content to the MMCU.

If not selected, the system considers all MCUs within the MCU pool order when starting a conference. However, even if the system selects an MMCU configured with an RDP translator, RDP content will not be delivered to or from Skype clients.

If an MCU failover occurs, video is automatically reconnected, but content is not re-established. The Skype conference or client must re-initiate content.

**Note:** This option can be used in place of a separate Polycom® ContentConnect™ gateway solution.

### Polycom MCU Video Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable MS RDP content</td>
<td>When selected, the RealPresence DMA system starts conferences based on this template only on Modular MCUs (MMCU) that have sufficient soft blade resources. MMCUs may be configured with an RDP translator that converts H.264 content shared from a standard endpoint to RDP content to deliver to a Skype ASMCU. Likewise, when a Skype client shares RDP content, the RDP translator delivers H.264 content to the MMCU. If not selected, the system considers all MCUs within the MCU pool order when starting a conference. However, even if the system selects an MMCU configured with an RDP translator, RDP content will not be delivered to or from Skype clients. If an MCU failover occurs, video is automatically reconnected, but content is not re-established. The Skype conference or client must re-initiate content. <strong>Note:</strong> This option can be used in place of a separate Polycom® ContentConnect™ gateway solution.</td>
</tr>
<tr>
<td>Presentation mode</td>
<td>Enables a conference to change to lecture mode when the current speaker speaks for 30 seconds. When another participant starts talking, it returns to the previous video layout. Not available if Video switching or Same layout is selected, or if Telepresence mode is Yes.</td>
</tr>
<tr>
<td>Same layout</td>
<td>Forces the selected layout on all participants. Personal selection of the video layout is disabled. Not available if Presentation mode or Video switching is selected, or if Telepresence mode is Yes.</td>
</tr>
<tr>
<td>Lecturer view switching</td>
<td>When in lecture mode, enables the lecturer’s view to automatically switch among participants (if the number exceeds the number of windows in the layout) while the lecturer is talking. Not available if Same layout is selected or Telepresence mode is Yes.</td>
</tr>
<tr>
<td>Auto layout</td>
<td>Lets the system select the video layout based on the number of participants in conference. Clear the check box to select a specific layout (below). Not available if Video switching is selected or Telepresence mode is Yes.</td>
</tr>
<tr>
<td>Layout</td>
<td>With Auto layout unchecked, you can select the number and arrangement of video frames. Once you choose a layout, a small representation of it displays here. Not available if Video switching is selected.</td>
</tr>
</tbody>
</table>

Polycom, Inc. 230
### Telepresence mode

Support for telepresence conference rooms joining the conference:
- **Auto** (default) — A conference is automatically put into telepresence mode when a telepresence endpoint (RPX, TPX, ATX, or OTX) joins.
- **On** — Telepresence mode is on, regardless of whether a telepresence endpoint is present.
- **Off** — Telepresence mode is off, regardless of whether a telepresence endpoint is present.

The **Auto** setting is recommended.

**Note:** The system flag `ITP_CERTIFICATION` must be set to YES. See the information about system flags in the MCU's Administrator's Guide.

### Telepresence layout mode

Layout choices for telepresence conferences:
- **Manual** — Layout is controlled manually by a conference operator using the Multipoint Layout Application (MLA) interface.
- **Continuous Presence** — Tells the MLA to generate a multipoint view (standard or custom).
- **Room Switch** — Tells the MLA to use Voice Activated Room Switching (VARS). The speaker’s site is the only one seen by others.
- **Speaker Priority** — Ensures that the current speaker is always displayed in the video layout. The previous speakers are also displayed if there is room in the layout. In this mode, each endpoint in the conference reserves screens for displaying the active speaker in the largest video layout cell available.
- **Participants Priority** — Uses a dynamic video layout that includes as many participants as possible.

Not available if Telepresence mode is **No**. See the Polycom Multipoint Layout Application User Guide for more information about layouts.

### Polycom MCU Audio Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Echo suppression</strong></td>
<td>Enables the MCU to detect and suppress echo. Available only on MCUs with MPM+ or MPx cards.</td>
</tr>
<tr>
<td><strong>Keyboard noise suppression</strong></td>
<td>Enables the MCU to detect and suppress keyboard noise. Available only on MCUs with MPM+ or MPx cards.</td>
</tr>
<tr>
<td><strong>Audio clarity</strong></td>
<td>Improves the voice quality in conference of a PSTN endpoint. Available only on version 7 and newer Polycom MCUs.</td>
</tr>
<tr>
<td><strong>Mute participants except lecturer</strong></td>
<td>Enables the MCU to automatically mute all participants except the lecturer upon connection to the conference.</td>
</tr>
<tr>
<td><strong>NoiseBlock™ (MPx or newer)</strong></td>
<td>Enables the MCU to automatically detect and mute endpoints that have a noisy audio channel. Not available on MCUs with an MPM+ card.</td>
</tr>
<tr>
<td><strong>Speaker change threshold (seconds) (MPx or newer)</strong></td>
<td>Allows you to configure the amount of time the MCU requires a participant to speak continuously until becoming the speaker. The default <strong>Auto</strong> setting is 3 seconds.</td>
</tr>
</tbody>
</table>
### Polycom MCU Skins

Lets you choose the display appearance (skin) for conferences using this template.

Not available if **Telepresence** mode is Yes or **Video switching** is enabled.

### Polycom MCU Conference IVR

**Override default conference IVR service**

Links this template to the specific conference IVR service selected in the list below.

**Note:** The Polycom MCU conference IVR service is separate and distinct from the RealPresence DMA system’s SIP-only shared number dialing feature (see **Shared Number Dialing**).

For most purposes, this option should not be selected. That enables the system to choose one of two defaults, depending on whether callers need to be prompted for passcodes. If you do select this option, be sure the IVR service you select is appropriate for the users who will use this template. See your Polycom MCU documentation for information about conference IVR services.

**Conference IVR service**

The list contains the names of all the conference IVR services available on the currently connected MCUs. If an IVR service is only available on some of the connected MCUs, its entry shows how many of the MCUs have that IVR service (for instance, 2 of 3).

The system will put conferences using this template on the least used MCU that has the selected conference IVR service. If there are none, it falls back to the default conference IVR service.

**Conference requires chairperson**

Conferences based on this template don’t start until a chairperson joins (callers arriving earlier are placed on hold) and may end when the last chairperson leaves (depending on the MCU configuration).

This option is ignored if the user doesn’t have a chairperson passcode.

For enterprise users, chairperson passcodes can come from the Active Directory, but you can override the Active Directory value.

For local users, you can add or change chairperson passcodes when you create or edit the users.

**Note:** If this option is enabled and this template is used for a Polycom RealConnect™ conference, the Skype for Business presenter acts as the chairperson for that conference.

**Terminate conference after chairperson drops**

If this template is used for a conference with a chairperson passcode, the conference is terminated when the chairperson leaves the conference. A message is played to the remaining participants informing them that the chairperson has left the conference.

### Polycom MCU Site Names

**Display mode**

Overlays the endpoint display name on each video participant’s display in a Continuous Presence conference:

- **Auto** — Display site names only when the layout changes.
- **On** — Always display site names.
- **Off** — Do not display site names (default).

**Font size**

Controls the font size for the site name text. The default value is 12.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Color</td>
<td>Allows you to configure the site name font appearance. When you select one of the Polycom MCU Skins with a background image, there are more color choices available for selection.</td>
</tr>
<tr>
<td>Display position</td>
<td>Controls the position of the text within the video participant's display with preset or custom locations. The value changes to Custom if you use the Horizontal position or Vertical position sliders to change the position to one that is not defined by a preset value.</td>
</tr>
<tr>
<td>Horizontal position</td>
<td>Allows you to manually control the horizontal position of the site name text.</td>
</tr>
<tr>
<td>Vertical position</td>
<td>Allows you to manually control the vertical position of the site name text.</td>
</tr>
<tr>
<td>Background transparency</td>
<td>When you choose one of the Polycom MCU Skins with a background image, you can use this slider to control the transparency of the site name font background.</td>
</tr>
</tbody>
</table>

**Polycom MCU Recording**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Record conference             | The conference recording setting for this template:  
• Disabled — Recording isn’t available for conferences using this template.  
• Immediately — Recording starts automatically when the conference starts.  
• Upon Request — Recording can be initiated manually by the chairperson or an operator.  
Conference recording requires a Polycom RealPresence Media Suite or Polycom Capture Server recording system and an MCU that supports recording. |
| Dial out recording link       | Select a specific recording link or the MCU’s default. The list contains the names of all recording links available on the connected MCUs, with the number of MCUs that have the link shown in parentheses.  
Available only on version 7 and newer Polycom MCUs. |
| Audio only                    | Limits recording to the audio channel of the conference.                                                                                   |
| Indication of recording       | Displays a red dot recording indicator in the upper left corner of the video layout.  
Available only on version 7.1 and newer Polycom MCUs. |
| Play recording message (V8.4 or newer) | Available with version 8.4 or newer RealPresence Collaboration Server MCUs.                                                              |

**Polycom MCU Indications**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Position</td>
<td>Use the drop-down menu to set the display position of the indication icons group.</td>
</tr>
<tr>
<td>Recordings</td>
<td>Enables the Recording icon, which is displayed if a recording is in progress.</td>
</tr>
<tr>
<td>Media type indications</td>
<td></td>
</tr>
<tr>
<td>Audio participants</td>
<td>Select the check box to enable the Audio Participants icon.</td>
</tr>
<tr>
<td>Video participants</td>
<td>Select the check box to enable the Video Participants icon.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Display mode</td>
<td>Select a radio button to change when and for how long the MCU displays the Audio Participants and Video Participants icons.</td>
</tr>
<tr>
<td>Permanent</td>
<td>The MCU displays the icon permanently when audio or video participants are connected.</td>
</tr>
<tr>
<td>On participant join or leave</td>
<td>The MCU displays the icon only for a short time when the number of audio or video participants changes.</td>
</tr>
<tr>
<td>Duration</td>
<td>Allows you to select the length of time the icon is visible upon a participant joining or leaving.</td>
</tr>
<tr>
<td>Network Quality</td>
<td>Enables the MCU to display the Network Quality icon, which indicates the network quality for any individuals experiencing significant packet loss.</td>
</tr>
<tr>
<td><strong>Polycom MCU Message Overlay</strong></td>
<td></td>
</tr>
<tr>
<td>Enable</td>
<td>Enables or disables Message Overlay (disabled by default).</td>
</tr>
<tr>
<td>Content</td>
<td>Enter the message text. The message text can be up to 50 Unicode characters.</td>
</tr>
<tr>
<td>Font size</td>
<td>Click the arrows to adjust the font size of the message text. The default is 24 points. Note: In some languages, for example Russian, when a large font size is selected, both rolling and static messages may be truncated if the message length exceeds the resolution width.</td>
</tr>
<tr>
<td>Color</td>
<td>Select the color and background of the message text. The default is white text on a red background.</td>
</tr>
<tr>
<td>Vertical position</td>
<td>Move the slider to the right to move the vertical position of the displayed text downward within the Video Layout. Move the slider to the left to move the vertical position of the displayed text upward within the Video Layout.</td>
</tr>
<tr>
<td>Background transparency</td>
<td>Move the slider to the left to decrease the transparency of the background of the message text. A transparency of 0 indicates no transparency (solid background color). Move the slider to the right to increase the transparency of the background of the message text. A transparency of 100 indicates full transparency (no background color). The default is 50.</td>
</tr>
<tr>
<td>Display repetition</td>
<td>Click the arrows to increase or decrease the number of times that the text message display is to be repeated. The default is 3.</td>
</tr>
<tr>
<td>Display speed</td>
<td>Select whether the message is static or moves across the screen. If moving, choose the movement speed. The default speed is Slow.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Cisco Codian</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Floor and chair control | Specifies how much control conference participants may have:  
- Do not allow floor or chair control — Participants have no control.  
- Allow floor control only — A participant may “take the floor.” Everyone sees that participant’s video full-screen.  
- Allow floor and chair control — A participant may also “take the chair.” The chair can designate whose video everyone sees full-screen. The chair can also disconnect participants.  
This setting works only in H.323 conferences and only if H.243 Floor and Chair Control is enabled on the MCU. All endpoints must support H.243 chair control. |
| Automatic lecture mode (4.1) | Enables the MCU to put a conference into lecture mode, either immediately or after the speaker has been talking for the selected interval. In lecture mode, the lecturer (speaker) is displayed full-screen to the other participants. The lecturer sees the normal continuous presence view.  
Available only on Codian v4.1 MCUs. |
| Layout control via FECC/DTMF | Enables participants to change their individual layouts using far end camera control, with or without fallback to touchtone commands for endpoints that don’t support FECC.  
FECC without fallback is available only on Codian v4.1 MCUs. |
| Mute in-band DTMF (4.1) | Specifies whether the MCU mutes participants’ in-band DTMF (touchtones) so that other participants don’t hear them:  
- When used for MCU control  
- Always  
- Never  
Available only on Codian version 4.1 MCUs. |
| Allow DTMF *6 to mute audio (4.1) | Enables conference participants to mute themselves using the *6 touchtone command.  
Available only on Codian version 4.1 MCUs. |
| Content channel video | Enables the conference to support a second video stream for content.  
This setting works only if Content Status is enabled on the MCU. |
| Transmitted content resolutions (4.1) | Specifies the aspect ratio used for the content channel. If Allow all resolutions is selected, endpoints with a 16:9 aspect ratio receive that, and others receive 4:3.  
Available only on Codian v4.1 MCUs. |
| Conference custom layout | Enables the Conference layout desired setting, where you can select the number and arrangement of video frames by clicking the image. |
| Conference layout desired | With Conference custom layout enabled, allows you to select the number and arrangement of video frames by clicking the image. Once a layout is chosen, a small representation of it appears here. See Select a Video Frames Layout. |

3 Click OK.
Select a Video Frames Layout

In the Select Layout dialog, you can select a specific conference layout when you’re adding or editing a conference template.

To select a video frames layout:

1. Click the radio button next to the layout you want.
2. Click OK.

Working with Conference Templates

The following sections describe the conference templates tasks you can perform.

View the Conference Templates List

On the Conference Templates page, you can view the current list of conference templates configured on the system.

To view the Conference Templates list:

» Go to Service Config > Conference Manager Settings > Conference Templates.
   The Conference Templates list appears.

Add a Standalone Conference Template

You can add a standalone conference template, which is a conference template that is not linked to a Polycom MCU conference profile.

To add a standalone conference template:

1. Go to Service Config > Conference Manager Settings > Conference Templates.
2. In the Actions list, click Add.
3. In the Add Conference Template dialog, specify all the conference properties for this template:
   a. In Common Settings, enter an appropriate name and description.
   b. Complete the remaining sections as desired. See Add a Conference Template.
4. Click OK.
   The new template appears in the Conference Templates list.

Add a Linked Conference Template

You can add a linked conference template, which is a conference template that is linked to a Polycom MCU conference profile. The system allows you to choose conference profiles from MCUs that have been added to the system.
To add a linked conference template:

1. Go to Service Config > Conference Manager Settings > Conference Templates.
2. In the Actions list, click Add.
3. In the Add Conference Template dialog, specify all the conference properties for this template:
   a. In Common Settings, enter an appropriate name and description.
   b. Click the Polycom MCU General Settings tab.
   c. Check Use existing profile and select the one you want from the Polycom MCU profile name list.
      The list contains the profiles available on the Polycom MCUs that have been added to the Polycom RealPresence DMA system. If no MCUs have been added to the system, the list is disabled.
4. Click OK.
   The new template appears in the Conference Templates list.

**Edit a Conference Template**

On the Conference Templates page, you can make and save changes to an existing conference template.

To edit a conference template:

1. Go to Service Config > Conference Manager Settings > Conference Templates.
2. In the Conference Templates list, select the template of interest, and in the Actions list, click Edit.
3. In the Edit Conference Template dialog, edit the settings as desired. See Edit a Conference Template.
4. Click OK.
   The template changes appear in the Conference Templates list.

**Change a Conference Template’s Priority**

You can control the priority of conference templates. This allows you to tell the system which template it should use when a user is associated with more than one.

To change a conference template’s priority:

1. Go to Service Config > Conference Manager Settings > Conference Templates.
2. On the Conference Templates list, select the template whose priority you want to change.
3. In the Actions list, select Move Up or Move Down, depending on whether you want to increase or decrease the template’s priority ranking.
   When a user is associated with multiple templates, the system uses the highest priority template. Polycom recommends moving the system default template to the bottom of the list.
4. Repeat until the template has the desired ranking.
Delete a Conference Template

You can remove a conference template from the system.

To delete a conference template:

1. Go to Service Config > Conference Manager Settings > Conference Templates.
2. In the Conference Templates list, select the template you want to delete, and in the Actions list, click Delete.
3. When asked to confirm that you want to delete the template, click Yes.

Any conference rooms or enterprise groups that used the template are reset to use the system default template.
IVR Prompt Sets

A prompt set contains a set of media files (audio prompts and video slides) that provide the caller experience for a RealPresence DMA-controlled IVR service. The RealPresence DMA system comes with a factory default call flow and corresponding prompt set. You can customize the IVR experience (in terms of language or branding) associated with the call flow by installing custom prompt sets and creating RealPresence DMA-controlled VEQs that use those prompt sets (see Shared Number Dialing).

A prompt set is an archive (.zip) file containing:

- A directory, META-INF, containing a single file, MANIFEST.MF. This is a text file describing the prompt set. It contains name:value attribute pairs separated by newlines. Currently, the RealPresence DMA system checks the following attribute names for valid values:
  - **AppName** identifies the call flow associated with this prompt set. Currently, "dma7000" is the only valid value.
  - **Promptset** is the name of the prompt set. This value must be unique across all prompt set zip files.

The following example is a valid custom manifest file (note that a custom manifest file requires two carriage returns at the end of the file):

```plaintext
Manifest-Version: 1.0
Ant-Version: Apache Ant 1.9.3
Created-By: 1.6.0_21-b07 (Sun Microsystems Inc.)
AppName: dma7000
Promptset: custompromptset
```

*Note:* The manifest file must not contain the attribute names **Format** and **Language**.

- A collection of .wav and .jpg files with the individual audio prompts and video slides.

  The .wav files should be encoded in PCM 16 Khz 16-bit mono format, and the file names must be exactly the same as in the default prompt set. If a custom prompt set is missing the .wav file for a specific prompt in the call flow, the RealPresence DMA system substitutes the corresponding prompt from the factory default prompt set.

  The .jpg files should be 1920x1088 pixels, and the file names must be exactly the same as in the default prompt set. If a custom prompt set is missing a .jpg file, the RealPresence DMA system substitutes the corresponding one from the factory default prompt set.

*Note:* The RealPresence DMA system does not examine the contents of the media files to validate the format.
The call flow currently uses only one video slide, General_Slide.jpg. The following table lists the audio prompt files it uses.

<table>
<thead>
<tr>
<th>Prompt File Name</th>
<th>Prompt Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chairperson_Identifier.wav</td>
<td>For conference chairperson services, enter the chairperson password.</td>
</tr>
<tr>
<td></td>
<td>All other participants, please wait.</td>
</tr>
<tr>
<td>Chairperson_PIN_Invalid.wav</td>
<td>Invalid chairperson password.</td>
</tr>
<tr>
<td>Chairperson_PIN_Invalid_Retry.wav</td>
<td>Invalid chairperson password. Please try again.</td>
</tr>
<tr>
<td>Conference_Full.wav</td>
<td>The conference is full. You cannot join at this time.</td>
</tr>
<tr>
<td>Conference_Locked.wav</td>
<td>The conference is locked. You cannot join at this time.</td>
</tr>
<tr>
<td>Conference_NID.wav</td>
<td>Please enter the conference ID.</td>
</tr>
<tr>
<td>Conference_NID_Invalid.wav</td>
<td>Invalid conference ID.</td>
</tr>
<tr>
<td>Conference_NID_Invalid_Retry.wav</td>
<td>Invalid conference ID. Please try again.</td>
</tr>
<tr>
<td>Conference_PIN.wav</td>
<td>Please enter the conference password.</td>
</tr>
<tr>
<td>Conference_PIN_Invalid.wav</td>
<td>Invalid conference password.</td>
</tr>
<tr>
<td>Conference_PIN_Invalid_Retry.wav</td>
<td>Invalid conference password. Please try again.</td>
</tr>
<tr>
<td>Disconnect.wav</td>
<td>You will now be disconnected.</td>
</tr>
<tr>
<td>General_Welcome.wav</td>
<td>Welcome to unified conferencing.</td>
</tr>
<tr>
<td>No_Resources_Available.wav</td>
<td>Sorry, the system is full.</td>
</tr>
<tr>
<td>Operator_Transfer.wav</td>
<td>You will now be transferred to the operator.</td>
</tr>
<tr>
<td>Operator_Transfer_Cancelable.wav</td>
<td>Press any key to cancel.</td>
</tr>
</tbody>
</table>

**View an IVR Prompt Set**

You can view current IVR prompt sets and details about the included prompts.

**To view the current IVR prompt sets:**

1. Go to Service Config > Conference Manager Settings > IVR Prompt Sets.
   The list of current IVR prompt sets displays.
2 Select an IVR prompt set to view detailed information about the included prompts. The Prompt Set Details pane displays information about the selected IVR prompt set.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prompt Set Details</td>
<td>Displays the following information about the selected prompt set:</td>
</tr>
<tr>
<td></td>
<td>• Prompt set and archive names.</td>
</tr>
<tr>
<td></td>
<td>• Application name (currently always dma7000).</td>
</tr>
<tr>
<td></td>
<td>• Archive checksum (to verify validity)</td>
</tr>
<tr>
<td></td>
<td>• Number of media files (.wav and .jpg) in the prompt set.</td>
</tr>
<tr>
<td>Included Media Status</td>
<td>Lists the media files in the prompt set, the IVR call flow, or both. The icon to the left shows the status of each. Hover over a file to see an explanation of the status.</td>
</tr>
</tbody>
</table>

Add a Custom IVR Prompt Set

You can add a custom Interactive Voice Response (IVR) prompt set and associate it with a Virtual Entry Queue.

To add a custom IVR prompt set:

1 Create an IVR prompt set zip file.

2 Go to Service Config > Conference Manager Settings > IVR Prompt Sets.

3 Under Actions, click Add IVR Prompt Set Archive.

4 Navigate to the file you want to use and click Open.

The system validates the Appname and Promptset values in the manifest file of the prompt set archive.
Shared Number Dialing

The RealPresence DMA system can be configured to handle SIP calls to certain shared numbers (virtual entry queues) by routing them to an appropriate Polycom MCU entry queue. Depending on the MCU type and version, Polycom MCUs can have two kinds of entry queues for providing callers with interactive voice response (IVR) services:

- **MCU-controlled entry queues** — The prompts, slides, and call flow providing the IVR experience reside on the MCU. Polycom MCUs refer to these as “IVR-only service provider” entry queues.
- **RealPresence DMA-controlled entry queues** (referred to as “External IVR control entry queues” on supporting MCUs because the IVR control is external to the MCU) — The prompts, slides, and call flow providing the IVR experience reside on the RealPresence DMA system (see IVR Prompt Sets).

A virtual entry queue (VEQ) connected to either type of MCU entry queue enables you to publicize a shared number that can be used to reach multiple virtual meeting rooms (VMRs), local RealConnect™ conferences, or RealConnect™ conferences hosted on external Skype for Business systems. When a caller dials the shared number, the RealPresence DMA system routes the call to an MCU with the resources and capability to provide the IVR experience associated with the shared number.

The shared number dialing call flow works as follows:

1. Callers dial a shared number to reach the Polycom RealPresence DMA system.
2. The Polycom RealPresence DMA system recognizes the dialed number as a VEQ number and routes the call to a Polycom MCU configured to provide the IVR experience (MCU-controlled or RealPresence DMA-controlled) that’s associated with the VEQ number dialed.

   **Note:** For RealPresence DMA-controlled VEQ numbers, the RealPresence DMA system recognizes two “speed dial” SIP dial string formats:

   - `<veq number>**<conference ID>` — The system validates the conference ID. If it’s valid, the caller bypasses the prompt for the destination conference. If the VMR has a conference passcode (PIN), chairperson passcode, or both, the system prompts for and validates the passcode.

   - `<veq number>**<conference ID>**<passcode>` — The system validates the conference ID, and if it’s valid, the passcode. If both are valid, the caller bypasses both prompts and is placed directly into conference.

3. If this is an MCU-controlled entry queue:
   a. The MCU uses its call flow, voice prompts, and video slides, prompting the caller for the conference ID of the destination conference and sending the response back to the Polycom RealPresence DMA system for validation.
   b. The Polycom RealPresence DMA system validates the conference ID entered by the caller. If the number is invalid, the RealPresence DMA system instructs the MCU to re-prompt the caller. The number of retries is configurable.
   c. If the caller entered a valid conference ID, the RealPresence DMA system routes the call to the conference (selecting an appropriate MCU and starting the conference if necessary). Prompting
for a passcode, if needed, is handled by the conference IVR service assigned to the conference template, if any, or the default conference IVR service.

4 If this is a RealPresence DMA-controlled entry queue:

a The Polycom RealPresence DMA system uses its call flow, voice prompts, and video slides, sending commands to the MCU to control the interaction with the caller (display slides, play prompts, collect tones, etc.).

b The Polycom RealPresence DMA system validates the conference ID entered by the caller.

   If the caller entered an invalid number, the RealPresence DMA system instructs the MCU to re-prompt the caller. The number of retries is configurable. If the caller fails to enter a valid number or enters the (configurable) operator request command, the RealPresence DMA system routes the call to the operator (help desk) SIP URI.

c If the conference has a conference passcode (PIN), chairperson passcode, or both, the RealPresence DMA system instructs the MCU to prompt for and collect the passcode. The RealPresence DMA system validates the passcode entered by the caller.

   If the caller entered an invalid passcode, the RealPresence DMA system instructs the MCU to re-prompt the caller. The number of retries is configurable. If the caller fails to enter a valid passcode or enters the (configurable) operator request command, the RealPresence DMA system routes the call to the operator (help desk) SIP URI.

d If the caller entered a valid passcode, the RealPresence DMA system routes the call to the conference (selecting an appropriate MCU and starting the conference if necessary), assigning the caller the appropriate role (chairperson or participant).

The default dial plan contains a dial rule that routes calls whose dialed number is a VEQ dial-in number to the correct VEQ.

You can create up to 60 different VEQs to provide different IVR experiences (for instance, different language prompts or different greetings). You can designate one of the MCU-controlled VEQs as the Direct Dial VEQ, and the system will use it for calls dialed without a VEQ or conference ID. For instance, if a call’s dial string includes only the system’s domain name or IP address, the Polycom RealPresence DMA system uses the Direct Dial VEQ for it.

For MCU-controlled VEQs, to create a unique experience, you must create the corresponding entry queue on the Polycom MCUs to be used.

For RealPresence DMA-controlled VEQs, the MCU’s entry queue must be one of its “External IVR Entry Queues.” The prompt set for the VEQ must be installed on the RealPresence DMA system (see IVR Prompt Sets). Different “External IVR Entry Queues” can be created on the MCUs to provide different profiles (bit rate, resolution, etc.) for the pre-conference phase, but most of the entry queue experience (language, prompts, retries, and timers) is defined by the RealPresence DMA-controlled VEQ.

**Note:** The entry queues created for shared number dialing VEQs must have the **IVR only service provider** setting selected. See your Polycom MCU documentation.

When selecting an MCU to handle IVR for a VEQ, the Polycom RealPresence DMA system chooses from among those that have the entry queue specified for that VEQ, without regard to MCU pool orders.

Ensure that the entry queue is available on the MCUs to be used and that it’s the same on each MCU.
View Virtual Entry Queues

You can view existing virtual entry queues (VEQs). The Shared Number Dialing page lists the VEQs available on the system and enables you to add, edit and delete VEQs.

To view virtual entry queues:

» Go to Service Config > Conference Manager Settings > Shared Number Dialing.

The following table describes the fields on the page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Entry Queue</td>
<td>The VEQ number, such as 12345, or Direct Dial.</td>
</tr>
<tr>
<td>Dial-In #</td>
<td>The complete dial string, for this VEQ. For instance, if the system uses the prefix 71, this might be 7112345.</td>
</tr>
<tr>
<td>Description</td>
<td>Typically, a description of the IVR experience, such as which language is used.</td>
</tr>
<tr>
<td>Response Entry Attempts</td>
<td>The number of times a caller can enter an invalid VMR number before the system rejects the call.</td>
</tr>
<tr>
<td>Polycom MCU Entry Queue</td>
<td>The name of the Polycom MCU entry queue (IVR experience) to be used for callers to this VEQ.</td>
</tr>
<tr>
<td>Entry Queue Type</td>
<td>Type of entry queue.</td>
</tr>
<tr>
<td>IVR Prompt Set</td>
<td>For a RealPresence DMA-controlled VEQ, the name of the IVR prompt set the VEQ uses.</td>
</tr>
</tbody>
</table>

Add a Virtual Entry Queue

You can add a virtual entry queue (VEQ) to the list of configured VEQs.

To add a virtual entry queue:

1. Go to Service Config > Conference Manager Settings > Shared Number Dialing.
2. Under Actions, click Add Virtual Entry Queue.
3. Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Entry Queue</td>
<td>The VEQ number.</td>
</tr>
<tr>
<td>Dial-in number</td>
<td>Number used to dial into the VEQ. Automatically set to the dialing prefix in Conference Settings, plus VEQ number.</td>
</tr>
<tr>
<td>Description</td>
<td>A meaningful description for this VEQ and its IVR experience, such as which language is used.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Response entry attempts</td>
<td>The number of times a caller can enter an invalid VMR number before the system rejects the call.</td>
</tr>
<tr>
<td>Polycom MCU entry queue</td>
<td>The Polycom MCU entry queue to use for this VEQ. The list includes all entry queues available on the Polycom MCUs connected to the system, with the number of MCUs that have each entry queue shown in parentheses. Note: Polycom MCUs refer to entry queues designed for a RealPresence DMA-controlled VEQ as “External IVR” because RealPresence DMA-based IVR control is external to the MCU.</td>
</tr>
<tr>
<td>Unique external Skype system</td>
<td>Instructs the system to attempt to resolve DTMF as a Skype conference ID for a specific external Skype for Business system. If this option is off, the system attempts to match the incoming DTMF against all defined external Skype for Business systems. If this option is on, the system attempts to match the incoming DTMF against the specific external Skype for Business system you choose from the list. If a match is found, the appropriate dial rule is executed. If the selected unique external Skype for Business system does not exist in the dial rule’s Selected external Skype systems box, the dial rule fails and the next dial rule is tried.</td>
</tr>
</tbody>
</table>

DMA-based IVR Call Flow (only for “External IVR control” entry queues)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid DTMF responses to conference ID prompt</td>
<td>The values a caller can enter when responding to a prompt for a conference ID: Conference room ID (VMR) Conference room alias RealConnect™ conference ID</td>
</tr>
<tr>
<td>IVR prompt set</td>
<td>For a RealPresence DMA-controlled VEQ, the prompt set to be used. The list includes all those installed on the RealPresence DMA system.</td>
</tr>
<tr>
<td>Timeout for response entry</td>
<td>The length of time that the RealPresence DMA system waits for a caller to respond to a prompt (5-60 seconds).</td>
</tr>
<tr>
<td>DTMF terminator</td>
<td>The terminator used to mark the end of caller input.</td>
</tr>
<tr>
<td>Operator assistance URI</td>
<td>The SIP URI to which to route the call for operator (help desk) assistance.</td>
</tr>
<tr>
<td>Request operator transfer DTMF</td>
<td>The DTMF command for requesting an operator. Note: If this digit string matches a VMR number, that VMR becomes unreachable.</td>
</tr>
<tr>
<td>Timeout to cancel operator request</td>
<td>The length of time after requesting an operator that a caller is given to cancel that request (1-10 seconds). Note: An operator request can be canceled by entering any DTMF key.</td>
</tr>
</tbody>
</table>

Script

Scripts entered in this section have access to the DTMF digits entered by callers. The system executes these scripts during VEQ processing, and can change and reject the DTMF digits callers enter. You can use this functionality to strip prefixes entered by a caller or to authorize participants dialing in to VEQs. These scripts are written in the Javascript language. Sample Virtual Entry Queue Script provides an example VEQ script that you can modify for your own purposes.
Add a Direct Dial Virtual Entry Queue

You can add a direct dial virtual entry queue (VEQ) to the list of configured VEQs.

To add a direct dial virtual entry queue:

1. Go to Service Config > Conference Manager Settings > Shared Number Dialing.
2. In the Actions pane, click Add Direct Dial Virtual Entry Queue.
3. Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>A description for this VEQ and its IVR experience, such as Direct Dial - English.</td>
</tr>
<tr>
<td>Response entry attempts</td>
<td>The number of times a caller can enter an invalid VMR number before the system rejects the call.</td>
</tr>
<tr>
<td>Polycom MCU entry queue</td>
<td>The Polycom MCU entry queue to use for this VEQ. The list includes all entry queues available on the Polycom MCUs connected to the system, with the number of MCUs that have each entry queue shown in parentheses.</td>
</tr>
<tr>
<td>Unique external Skype system</td>
<td>Instructs the system to attempt to resolve DTMF as a Skype conference ID for a specific external Skype for Business system. If this option is off, the system attempts to match the incoming DTMF against all defined external Skype for Business systems. If this option is on, the system attempts to match the incoming DTMF against the specific external Skype for Business system you choose from the list. If a match is found, the appropriate dial rule is executed. If the selected unique external Skype for Business system does not exist in the dial rule’s Selected external Skype systems box, the dial rule fails and the next dial rule is tried.</td>
</tr>
</tbody>
</table>

4. Click OK.

Edit a Virtual Entry Queue

You can edit a virtual entry queue (VEQ) as needed.

To edit a direct dial virtual entry queue:

1. Go to Service Config > Conference Manager Settings > Shared Number Dialing.
2. Select the virtual entry queue of interest and click **Edit Virtual Entry Queue**.

3. Revise the following fields as needed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Virtual Entry Queue</strong></td>
<td></td>
</tr>
<tr>
<td>Virtual entry queue number</td>
<td>The VEQ number.</td>
</tr>
<tr>
<td>Dial-in number</td>
<td>Number used to dial into the VEQ. Automatically set to the dialing prefix in Conference Settings, plus VEQ number.</td>
</tr>
<tr>
<td>Description</td>
<td>A meaningful description for this VEQ and its IVR experience, such as which language is used.</td>
</tr>
<tr>
<td>Response entry attempts</td>
<td>The number of times a caller can enter an invalid VMR number before the system rejects the call.</td>
</tr>
<tr>
<td>Polycom MCU entry queue</td>
<td>The Polycom MCU entry queue to use for this VEQ. The list includes all entry queues available on the Polycom MCUs connected to the system, with the number of MCUs that have each entry queue shown in parentheses. <strong>Note:</strong> Polycom MCUs refer to entry queues designed for a RealPresence DMA-controlled VEQ as “External IVR” because RealPresence DMA-based IVR control is external to the MCU.</td>
</tr>
<tr>
<td>Unique external Skype system</td>
<td>Instructs the system to attempt to resolve DTMF as a Skype conference ID for a specific external Skype for Business system. If this option is off, the system attempts to match the incoming DTMF against all defined external Skype for Business systems. If this option is on, the system attempts to match the incoming DTMF against the specific external Skype for Business system you choose from the list. If a match is found, the appropriate dial rule is executed. If the selected unique external Skype for Business system does not exist in the dial rule's <strong>Selected external Skype systems</strong> box, the dial rule fails and the next dial rule is tried.</td>
</tr>
</tbody>
</table>

**DMA-based IVR Call Flow (only for “External IVR control” entry queues)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Valid DTMF responses to conference ID prompt | The values a caller can enter when responding to a prompt for a conference ID:  
  Conference room ID (VMR)  
  Conference room alias  
  RealConnect™ conference ID  
  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| IVR prompt set                             | For a RealPresence DMA-controlled VEQ, the prompt set to be used. The list includes all those installed on the RealPresence DMA system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Timeout for response entry (sec)           | The length of time that the RealPresence DMA system waits for a caller to respond to a prompt (5-60 seconds).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| DTMF terminator                            | The terminator used to mark the end of caller input.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Operator assistance URI                    | The SIP URI to which to route the call for operator (help desk) assistance.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Request operator transfer DTMF             | The DTMF command for requesting an operator. **Note:** If this digit string matches a VMR number, that VMR becomes unreachable.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
Edit a Direct Dial Virtual Entry Queue

You can edit a direct dial virtual entry queue (VEQ) when necessary.

To edit a virtual entry queue:

1. Go to Service Config > Conference Manager Settings > Shared Number Dialing.
2. Select the direct dial virtual entry queue of interest and click Edit Direct Dial Virtual Entry Queue.
3. Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>A meaningful description for this VEQ and its IVR experience, such as Direct Dial - English.</td>
</tr>
<tr>
<td>Response entry attempts</td>
<td>The number of times a caller can enter an invalid VMR number before the system rejects the call.</td>
</tr>
<tr>
<td>Polycom MCU entry queue</td>
<td>The Polycom MCU entry queue to use for this VEQ. The list includes all entry queues available on the Polycom MCUs connected to the system, with the number of MCUs that have each entry queue shown in parentheses.</td>
</tr>
<tr>
<td>Unique external Skype system</td>
<td>Instructs the system to attempt to resolve DTMF as a Skype conference ID for a specific external Skype for Business system.</td>
</tr>
<tr>
<td></td>
<td>If this option is off, the system attempts to match the incoming DTMF against all defined external Skype for Business systems.</td>
</tr>
<tr>
<td></td>
<td>If this option is on, the system attempts to match the incoming DTMF against the specific external Skype for Business system you choose from the list. If a match is found, the appropriate dial rule is executed. If the selected unique external Skype for Business system does not exist in the dial rule’s Selected external Skype systems box, the dial rule fails and the next dial rule is tried.</td>
</tr>
</tbody>
</table>
Test Script Debugging for VEQ Scripts

You can test a Javascript executable script that you’ve associated with a Virtual Entry Queue (VEQ). It lets you specify parameters of a call and the DTMF string entered by a caller, observing the result of the script.

To test script debugging for VEQ scripts:

1. Navigate to Service Config > Conference Manager Settings > Shared Number Dialing.
2. In the Actions pane, click Edit Virtual Entry Queue.
3. In the Edit Virtual Entry Queue dialogue, select Scripts.

The following table describes the fields in the dialog.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dial string</td>
<td>This is the DIAL_STRING variable in the script. Enter a dial string if script execution depends on this variable. Alternatively, provide the entire SIP INVITE message. Note: For SIP, the script should always specify the schema prefix (sip or sips). For instance: DIAL_STRING = &quot;sip:xxx@10.33.120.58&quot;</td>
</tr>
<tr>
<td>DTMF digits</td>
<td>Enter the DTMF digits, corresponding to the script variable DTMF_STRING, that should be evaluated or transformed by the script.</td>
</tr>
<tr>
<td>Caller site</td>
<td>Select a site in order to set the first four caller variables.</td>
</tr>
<tr>
<td>Caller variables</td>
<td>Lists variables that can be used in the script to represent caller alias values. Enter an alias value to test for that variable.</td>
</tr>
<tr>
<td>Final result</td>
<td>Displays the outcome of running the script. If the script rejected the DTMF string, a message tells you so. Otherwise, the transformed DTMF string is displayed.</td>
</tr>
<tr>
<td>Script output</td>
<td>Displays any output produced by the script (e.g., println statements).</td>
</tr>
<tr>
<td>Output SIP headers</td>
<td>Displays any SIP headers produced by the script.</td>
</tr>
</tbody>
</table>

4. Complete the required fields and click Debug this Script.

Sample Virtual Entry Queue Script

Virtual Entry Queue (VEQ) scripts are scripts written in the Javascript language that have access to the DTMF digits entered by callers. The system executes these scripts during VEQ processing, and can change and reject the DTMF digits callers enter. You can use this functionality to strip prefixes entered by a caller or to authorize participants dialing in to VEQs.

VEQ scripts have access to the DTMF_STRING variable.
You can use `return ACCEPT;` and `return REJECT;` statements to accept or reject the entered DTMF digits. When you `return ACCEPT;`, the script accepts the entered DTMF digits as is. When you `return REJECT;`, the system does not accept the DTMF digits and prompts the caller again for new DTMF input.

The following sample script shows how to use the scripting feature to restrict participants calling a specific VEQ to a whitelist of VMRs.

```
var whitelist_vmrs = [
  "1000",    // Specify list of VMRs; add or remove VMRs from this list.
  "2000",    // Make sure you use the syntax "<vmr number>"<comma>
  "3000",
];

var whitelist_patterns = [
  "^44",    // The ^ causes the pattern match at the beginning of the string.
  "^76"     // So 441000 will match but 100044 will not.
];
```

```
// Match against individual VMRs. ACCEPT if any of them matches.
if (0 <= whitelist_vmrs.indexOf(DTMF_STRING))
{
  return ACCEPT;
}
```

```
// Match against patterns. ACCEPT if any of them matches.
for (i=0; i<whitelist_patterns.length; i++)
{
  if (DTMF_STRING.match(whitelist_patterns[i]))
  {
    return ACCEPT;
  }
}
```

`return REJECT;`
SIP Conference Factories

SIP conference factories enable users on some brands and models of endpoints to escalate a point-to-point call to an ad-hoc, multi-party conference call on a Polycom MCU. SIP conference factories create conferences based on a dial rule with the action to resolve to a SIP conference factory.

Working with SIP Conference Factories

Users with certain brands and models of endpoints (known as escalating endpoints) can escalate multiple point-to-point calls to a RealPresence DMA conference by calling a SIP conference factory. When the RealPresence DMA system receives an incoming call from an escalating endpoint to a SIP conference factory, the system creates a dynamic multi-point conference on an MCU and generates a conference ID for the conference. The conference IDs are strings that can be dialed by any endpoint (SIP or H.323) to join the conference. These conference IDs are not VMR IDs and the conferences do not have associated VMRs.

Once the RealPresence DMA system creates the dynamic conference, the escalating endpoint invites itself to the conference and then transfers (refers) its calls with other endpoints into the multi-point conference. Any user attending the conference can then invite other participants by providing them with the conference ID.

Unlike VMR conferences, SIP conference factory conferences are not associated with individual RealPresence DMA users and are not included in queries of VMRs. SIP conference factory conferences are resolvable by the test dial rules feature.

The RealPresence DMA system provides a pre-configured SIP conference factory with the SIP conference factory ID \textbf{plcm-scf}. You can edit this SIP conference factory as needed or delete it. This default SIP conference factory creates conferences using the default conference template, the default MCU pool order, in the default territory within the system’s site topology.

The RealPresence DMA system default dial plan includes the dial rule \textbf{Dial to SIP conference factory} that you can enable to support SIP conference factories.

Any number of dial rules with the action to \textbf{Resolve to SIP conference factory} may be included in a dial plan.

Add a SIP Conference Factory

You can add SIP conference factories in the RealPresence DMA system to support escalation of point-to-point calls to multi-point calls.

To add a SIP conference factory

1. Go to Service Config > Conference Manager Settings > SIP Conference Factories.
2 Click Add.
3 Select Enabled.
4 Complete the fields described in the following table as needed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>A brief description of the SIP conference factory.</td>
</tr>
<tr>
<td>Conference Factory ID*</td>
<td>The unique ID of the SIP conference factory. This is the dial string that invokes the SIP conference factory.</td>
</tr>
<tr>
<td></td>
<td>Conference Factory IDs must meet the following requirements in order to be valid:</td>
</tr>
<tr>
<td></td>
<td>• Must start and end with an alphanumeric character.</td>
</tr>
<tr>
<td></td>
<td>• Characters in the middle may be alphanumeric or any of the following:</td>
</tr>
<tr>
<td></td>
<td>_ ~ ! $ &amp; , . ’ = + - * ( )</td>
</tr>
<tr>
<td></td>
<td>% is allowed only if it is followed by at least two alphanumeric characters.</td>
</tr>
<tr>
<td></td>
<td>• Cannot contain blank spaces.</td>
</tr>
<tr>
<td>Conference Template</td>
<td>The conference template that defines the properties of a SIP conference factory conference.</td>
</tr>
<tr>
<td></td>
<td>Defaults to the conference template configured in Conference Settings.</td>
</tr>
<tr>
<td>MCU Pool Order</td>
<td>The MCU pool order that specifies the order in which the MCU pools are used.</td>
</tr>
<tr>
<td></td>
<td>Defaults to the MCU pool order configured in Conference Settings.</td>
</tr>
<tr>
<td>Territory</td>
<td>The territory assigned to a SIP conference factory conference room if it isn’t specified at the conference room level.</td>
</tr>
</tbody>
</table>

5 Click OK.

**Edit a SIP Conference Factory**

You can edit SIP conference factory settings as needed in the RealPresence DMA system to support escalation of point-to-point calls to multi-point calls. You can also disable a SIP conference factory without deleting it.

**To edit a SIP conference factory**

1 Go to Service Config > Conference Manager Settings > SIP Conference Factories.
2 Select the SIP conference factory to revise and click Edit.
3 Do one of the following:
   1 Select Enabled to activate the SIP conference factory.
   2 Clear the Enabled check box to disable the SIP conference factory without deleting it.
4 Revise the fields described in the following table as needed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>A brief description of the SIP conference factory.</td>
</tr>
<tr>
<td>Conference Factory ID*</td>
<td>The unique ID of the SIP conference factory. This is the dial string that invokes the SIP conference factory. Conference Factory IDs must meet the following requirements in order to be valid: • Must start and end with an alphanumeric character. • Characters in the middle may be alphanumeric or any of the following: _ ~ ! $ &amp; , . ’ = + - * ( ) % is allowed only if it is followed by at least two alphanumeric characters. • Cannot contain blank spaces.</td>
</tr>
<tr>
<td>Conference Template</td>
<td>The conference template that defines the properties of a SIP conference factory conference. Defaults to the conference template configured in Conference Settings.</td>
</tr>
<tr>
<td>MCU Pool Order</td>
<td>The MCU pool order that specifies the order in which the MCU pools are used. Defaults to the MCU pool order configured in Conference Settings.</td>
</tr>
<tr>
<td>Territory</td>
<td>The territory assigned to a SIP conference factory conference room if it isn’t specified at the conference room level.</td>
</tr>
</tbody>
</table>

5 Click OK.

**Delete a SIP Conference Factory**

You can delete a SIP conference factory if it will no longer be used.

**To delete a SIP conference factory**

1 Go to Service Config > Conference Manager Settings > SIP Conference Factories.
2 Select the SIP conference factory to delete and click Delete.
3 Click Yes to confirm the deletion.
Presence Publishing for Skype

The RealPresence DMA system allows you to integrate with Microsoft® Skype for Business environments. When you integrate the RealPresence DMA system into a Skype environment, the system communicates with the Skype servers and Active Directory to provide contact presence and conference interaction between MCUs managed by the RealPresence DMA system and the Skype AVMCU. Presence allows Skype clients to view the presence of a RealPresence DMA system VMR, similar to any other contact in the Skype client contact list.

Configure Presence Publishing for Skype

If your Polycom RealPresence DMA system is integrated with a Microsoft® Skype for Business environment, you can configure system-wide default settings related to presence publishing for Polycom conference contacts.

Before you configure presence publishing, confirm that your RealPresence DMA system's identity certificate contains accurate information. An incorrect certificate may cause an error when the RealPresence DMA system attempts to contact the Skype for Business server to update the presence status.

To configure presence publishing for Skype:

2. Complete the fields described in the following table as needed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Publish presence for Polycom         | When checked, presence status for each conference contact is visible in the Skype for Business contact window.  
                                        | conference contacts                                                                                                                        |
|                                       | **Note:** This check box affects the option Default Polycom conference contacts presence settings.                                               |
| Skype pool to create/publish to      | A list of Microsoft SIP peer pools to which the RealPresence DMA system can publish presence. Select the pool whose clients should see presence  |
|                                       | indications for conference contacts.  
                                        | A Skype pool will appear in the list if:  
                                        | • The pool is defined as an **External SIP Peer** with a type of **Microsoft**.  
                                        | • The field **Maximum Polycom conference contacts to publish** in the **External SIP Peer Skype Integration** tab is set to a value greater than  |
|                                       | zero.                                                                                                                                       |
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact SIP domain*</td>
<td>The domain portion of the SIP URI that the RealPresence DMA system uses for a conference contact (for example, sipdomain.net). The conference contacts are created in this domain. If the domain does not exist, it will be created if the <strong>Create Polycom conference contacts</strong> check box is enabled. <strong>Note</strong>: If there are multiple superclusters that are integrated with a Skype for Business environment, this field should be different for each supercluster. If this value is the same across multiple superclusters and the systems are integrated with the same Active Directory, settings changes on one supercluster could affect other superclusters. When you enable the <strong>Publish presence for Polycom conference contacts</strong> check box and <strong>Update</strong> the settings, a warning may display.</td>
</tr>
<tr>
<td>Create Polycom conference contacts</td>
<td>Only available if Microsoft Active Directory integration is enabled. When checked, the RealPresence DMA system will create Active Directory resources for any meeting rooms that have the <strong>Presence</strong> option enabled. If you have not changed the <strong>Presence</strong> option manually for any VMRs, all VMRs will have corresponding Active Directory contacts created.</td>
</tr>
<tr>
<td>VMR display name pattern</td>
<td>The text pattern that describes the name of the VMR contact. This text will precede the VMR number when displayed in the Skype contact window (for example, a VMR display name pattern of “Conference room” would create display names of “Conference room &lt;VMR number&gt;”). The maximum pattern length is 63 characters. After you edit this field, it may take some time for the change to be seen in the Skype client, depending on how many conference contacts the RealPresence DMA system is managing.</td>
</tr>
<tr>
<td>OU for contacts</td>
<td>The Active Directory OU (Organizational Unit) in which the RealPresence DMA system should create contact resources. If left blank, the system creates resources in the CN=Users container.</td>
</tr>
<tr>
<td>Default Polycom conference contacts</td>
<td>Changes the default system-wide setting for VMR presence publishing and Active Directory contact creation. Depending on the settings of the <strong>Publish presence for Polycom conference contacts</strong> and <strong>Create Polycom conference contacts</strong> options, there are two modes of operation for this field. See step 3 to complete this field. <strong>Note</strong>: The setting in this field can be overridden by other presence settings in the system.</td>
</tr>
<tr>
<td>presence settings</td>
<td></td>
</tr>
</tbody>
</table>
3 Select the **Default Polycom conference contacts presence settings** based on the following information:

<table>
<thead>
<tr>
<th>Publish presence for Polycom conference contacts</th>
<th>Create Polycom conference contacts</th>
<th>Default Polycom conference contacts presence settings</th>
</tr>
</thead>
</table>
| Checked                                          | Unchecked                         | • Publish Polycom conference contacts presence  
|                                                 |                                   | • Do not publish Polycom conference contacts presence |

| Checked | Checked | • Create Polycom conference contacts and publish presence  
|         |         | • Do not create Polycom conference contacts or publish presence |

4 Click **Update** to save the settings.

**Remove Contacts from Active Directory**

If you disable the **Publish presence for Polycom conference contacts** option and Active Directory integration is enabled, the **Remove Contacts from Active Directory** action becomes available in the left-hand navigation pane. For systems integrated with a Microsoft® Skype for Business environment, this action allows you to remove any contacts in Active Directory created by the RealPresence DMA system.

Removing contacts will apply to contacts created by any supercluster integrated with the Active Directory.

If you remove all contacts across all SIP domains, the conference contacts associated with other RealPresence DMA system superclusters that were removed will be automatically recreated daily when the systems sync with Active Directory. You can also manually recreate these contact resources.

**To remove contacts from Active Directory:**

1 Go to **Service Config > Conference Manager Settings > Presence Publishing for Skype.**
2 Uncheck **Publish presence for Polycom conference contacts.**
3 Click **Update.**
4 Click **Remove Contacts from Active Directory** and choose one of the following options:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove all Polycom conference contacts associated with contact SIP domain</td>
<td>Limit the change to one SIP domain. The default value in the text field is the current SIP domain in the <strong>Contact SIP domain</strong> field.</td>
</tr>
<tr>
<td>Remove all Polycom conference contacts associated with any contact SIP domain</td>
<td>All conference contacts created by the RealPresence DMA system are removed, regardless of SIP domain.</td>
</tr>
</tbody>
</table>

5 Click **Update.**
Recreate Skype Contact Resources

You can manually recreate Microsoft® Skype for Business contact resources associated with other superclusters.

To manually recreate Skype contact resources associated with other superclusters:
1. Log in to a system on one of the affected superclusters.
2. Go to Service Config > Conference Manager Settings > Presence Publishing for Skype.
3. Uncheck Publish presence for Polycom conference contacts.
4. Click Update.
5. Select Publish presence for Polycom conference contacts.
6. Click Update.
   A caution dialog may appear regarding contact SIP domains for multiple superclusters.
7. Click OK.
8. Repeat the preceding steps for any other affected superclusters.
Call Server Configuration

This section provides an introduction to configuring the Polycom® RealPresence® DMA® system’s Call Server. It includes:

- Call Server Settings
- Dial Plans
- Prefix Service
- Hunt Groups
- Domains Restrictions
- Preliminary and Postliminary Scripting
Call Server Settings

The Polycom RealPresence DMA system's Call Server capabilities provide gatekeeper functionality (if H.323 signaling is enabled), SIP proxy server and registrar functionality (if SIP signaling is enabled), and bandwidth management. The system can also function as an H.323 <-> SIP gateway.

The RealPresence DMA system's gateway function is used only for calls to registered endpoints, SIP peers, and H.323 gatekeepers. It is not used for calls to virtual meeting rooms (VMRs), virtual entry queues (VEQs), external IP addresses.

In H.323, DTMF tones are usually sent over the H.323 signaling path. In SIP, DTMF tones are usually sent over the media path as a special RTP payload packet (see RFC 4733). Because of this difference and because the RealPresence DMA system is not in the media path, its gateway function does not support DTMF transmission.

The gateway function also does not support content sharing or AES encryption.

Configure the Call Server

The gatekeeper and SIP proxy settings used by the call server apply to all of the clusters in a supercluster.

To configure the call server:

1. Go to Service Config > Call Server Settings.
2. Configure the call server settings as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Settings</td>
<td></td>
</tr>
<tr>
<td>Allow calls to/from rogue endpoints</td>
<td>If this option is selected, the Call Server permits rogue endpoints to place and receive calls. Rogue endpoints are endpoints that are in sites managed by the system, but are not registered and active. Turning this option off blocks calls from and to rogue endpoints. This option has no effect on other unregistered network devices (such as MCUs, gatekeepers, and Session Border Controllers) or on endpoints that are not in sites managed by the system.</td>
</tr>
</tbody>
</table>
### Field | Description
---|---
Allow calls to inactive endpoints | If this option is selected, the Call Server considers inactive as well as active endpoints when attempting to resolve an address using the *Dial registered endpoints by alias* dial rule. Turning this option off can prevent the aliases of registrations that are no longer active from masking the aliases of endpoints registered to other call servers. This is useful in situations where an endpoint might have an active registration with one Call Server and an inactive registration with another (such as a mobile device that moves from a Call Server handling registrations through an SBC to a different Call Server in the network).

Available bandwidth limit (percent) | Sets the maximum percentage of the available bandwidth that can be allocated to a single call. If the requested bandwidth exceeds this value, the Call Server “downspeeds” (reduces the bit rate of) the call, but only to the user’s downspeed minimum. If there is insufficient bandwidth to comply with both this setting and the downspeed minimum, the call is rejected.

Territory failover delay (seconds) | The number of seconds a territory’s backup cluster waits after losing contact with the primary before it takes over the territory. Must be in the range 6-300.

Timeout for call forwarding when no answer (seconds) | The number of seconds to wait for the called endpoint to answer (fully connect) before forwarding the call, if call forwarding on no answer is enabled for the called endpoint. Must be in the range 5-32.

Registration refresh interval (seconds) | For H.323 endpoints, specifies how often registered endpoints send keep alive messages to the Call Server. Endpoints that fail to send keep alive messages on time are flagged as inactive. For SIP endpoints, specifies the refresh interval used if the endpoint didn’t specify an interval or specified one greater than this value. Must be greater than or equal to the minimum SIP registration interval and in the range 150-9999.

Skype conference ID query timeout (seconds) | When integrated with a Microsoft® Skype® for Business environment, limits the duration of queries to the Skype for Business server for a dialed conference ID. Must be in the range 1-20.

Bit rate to bandwidth conversion factor | The factor used to derive the bandwidth needed for a call from a specified bit rate. You can use any value from 1.000 to 5.000 (the system supports up to three decimal places of precision). This value not only affects site topology bandwidth limit calculations, but also affects bit rate and bandwidth statistics that the system reports for calls. **Note:** Before version 6.2, this value was 2.5 and not configurable. If you upgrade a system running software prior to version 6.2 to version 6.2 or later, the conversion factor remains at 2.5 after the upgrade (although it is now configurable). If you restore a pre-6.2 backup to a version 6.2 or later system, the conversion factor becomes the value configured in the backup you restore. **Note:** Bandwidth calculations for H.323 calls require that the hosting MCU be actively registered to the RealPresence DMA system.
For SIP calls gatewayed to an external gatekeeper, use the H.323 email ID as the destination

If this option is selected, when the system uses dial rules to attempt to resolve a SIP call to an external gatekeeper, the Call Server sets the destination in the LRQ message to the H.323 email ID (such as 1234@example.com) rather than utilizing the E.164 number alone (such as 1234). Some external gatekeepers, such as the RealPresence Access Director system, may need the additional domain information in the LRQ message to correctly resolve the LRQ request.

If this option is off, SIP calls gatewayed by the RealPresence DMA system to a RealPresence Access Director configured as an external H.323 gatekeeper fail because the gatekeeper doesn't have enough information to route the call.

Note: This option affects communications with all external H.323 gatekeepers to which the RealPresence DMA system gateways SIP calls.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>For SIP calls gatewayed to an external gatekeeper, use the H.323 email ID as the destination</td>
<td>If this option is selected, when the system uses dial rules to attempt to resolve a SIP call to an external gatekeeper, the Call Server sets the destination in the LRQ message to the H.323 email ID (such as <a href="mailto:1234@example.com">1234@example.com</a>) rather than utilizing the E.164 number alone (such as 1234). Some external gatekeepers, such as the RealPresence Access Director system, may need the additional domain information in the LRQ message to correctly resolve the LRQ request. If this option is off, SIP calls gatewayed by the RealPresence DMA system to a RealPresence Access Director configured as an external H.323 gatekeeper fail because the gatekeeper doesn't have enough information to route the call.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Settings</td>
<td>The minimum time between “keep alive” messages to SIP endpoints. Must be less than or equal to the registration refresh interval and in the range 150-3600.</td>
</tr>
<tr>
<td>Minimum SIP registration interval (seconds)</td>
<td>The minimum time between “keep alive” messages to SIP endpoints. Must be less than or equal to the registration refresh interval and in the range 150-3600.</td>
</tr>
<tr>
<td>SIP OPTIONS ping timer (seconds)</td>
<td>The frequency with which the system sends SIP OPTIONS requests when no other SIP traffic is received from the SIP peer. Must be in the range 1-10000. The default value is 10.</td>
</tr>
<tr>
<td>SIP OPTIONS ping failure status codes</td>
<td>Specifies which responses to the OPTIONS request indicate that a SIP peer is not responsive. Valid input is a comma-separated list or dash-separated range of three-digit numeric codes; an empty field is acceptable as well. The default value is 503.</td>
</tr>
<tr>
<td>SIP max breadth</td>
<td>The maximum number of SIP peers that the system will try at once. This option applies when the Routing policy for a dial rule with the action Resolve to external SIP peer is set to All in parallel (forking). Must be in the range 1-99. The default value is 60.</td>
</tr>
<tr>
<td>Try next SIP peer timeout (seconds)</td>
<td>The timeout in seconds when sending a SIP OPTIONS ping or an INVITE to a SIP peer. This value can be a numeric value in the range 0.1-31.0. The default value is 5.0.</td>
</tr>
<tr>
<td>SIP peer dial rule timeout (seconds)</td>
<td>The number of seconds after invoking the dial rule that the dial attempt is cancelled. Must be in the range 1-300. The default value is 25.</td>
</tr>
<tr>
<td>Nonresponsive SIP peer status codes</td>
<td>Specifies which responses to an initial SIP INVITE indicate that a SIP peer is not responsive. Valid input is a comma-separated list or dash-separated range of three-digit numeric codes; an empty field is acceptable as well. The default value is 503.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>H.323 Settings</strong></td>
<td><strong>Gatekeeper call mode</strong> — The Call Server processes only H.225.0 RAS call control messages. The endpoints exchange other call signaling and media control messages directly, bypassing the gatekeeper. <strong>Routed call mode</strong> — The Call Server proxies all H.323 signaling messages.</td>
</tr>
<tr>
<td><strong>Accept H.323 neighbor requests only from specified external gatekeepers</strong></td>
<td>If this option is selected, the Call Server accepts H.323 location requests (LRQs) only from gatekeepers configured on the <strong>External Gatekeeper</strong> page.</td>
</tr>
<tr>
<td><strong>Resolve H.323 Email-ID dial strings to other registered H.323 aliases</strong></td>
<td>If this option is selected, the Call Server resolves email ID dial strings to another local alias by using the user part of the email address. For example, the dial string <a href="mailto:1234@mycompany.com">1234@mycompany.com</a> would resolve to the endpoint registered as 1234.</td>
</tr>
<tr>
<td><strong>Automatically assign enterprise users’ email addresses as H.323 email IDs</strong></td>
<td>If this option is selected and the system is integrated with Active Directory, an endpoint associated with an enterprise user is assigned the user’s email address (if that address hasn’t already been explicitly assigned to another endpoint).</td>
</tr>
<tr>
<td><strong>Location request hop count</strong></td>
<td>The initial hop count the Call Server uses when it sends LRQs to neighbored gatekeepers.</td>
</tr>
<tr>
<td><strong>Location request timeout (seconds)</strong></td>
<td>The number of seconds to wait for a response from a neighbored gatekeeper.</td>
</tr>
<tr>
<td><strong>IRQ sending interval (seconds)</strong></td>
<td>The interval at which the system sends IRQ messages to H.323 endpoints in a call, requesting QoS (quality of service) reports. Must be in the range 10-600.</td>
</tr>
<tr>
<td><strong>Terminate calls based on failed responses to IRQs</strong></td>
<td>If this option is selected, the Call Server terminates a call if it sends an IRQ (Information Request) to an endpoint that signaled support for IRQs, and the endpoint either fails to respond or responds with an IRR (Information Request Response) containing an invalidCall field. This is the correct behavior according to the H.323 ITU Specification, and it prevents a call license from being used unnecessarily for a call that's no longer active. Some endpoints (VVX prior to v.4.0.1; Sony PCS1, XG80, and G70; and possibly others) signal support for IRQs but don’t properly handle IRQ/IRR messaging, causing active calls to be disconnected if this option is selected. To avoid this problem with such endpoints, leave this option off. <strong>Note:</strong> This setting has no effect on calls from endpoints that don’t signal support for IRQs.</td>
</tr>
<tr>
<td><strong>Dynamically blacklist signaling from hyperactive endpoints</strong></td>
<td>If this option is selected, the Call Server adds H.323 endpoints to its blacklist (ignoring their signaling messages) when they send duplicate RRQ or GRQ messages in excess of the criteria you specify below. When an endpoint is blacklisted, the Call Server: • Stops interpreting, responding to, auditing, or logging messages of that type from the endpoint. • Creates Alert 5003 and corresponding SNMP trap. • Logs the blacklisting.</td>
</tr>
</tbody>
</table>
### Gatekeeper Blacklist Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Message Type</strong></td>
<td>You can specify the blacklist settings separately for RRQ (Registration Request) and GRQ (Gatekeeper Request) messages.</td>
</tr>
<tr>
<td><strong>Threshold</strong></td>
<td>The number of duplicate messages within the specified interval that causes an endpoint to be blacklisted.</td>
</tr>
<tr>
<td><strong>Interval (msec)</strong></td>
<td>The interval in milliseconds to which the threshold applies.</td>
</tr>
<tr>
<td><strong>Quarantine</strong></td>
<td>If this option is selected, endpoints that are blacklisted are also quarantined. They remain in Quarantined or Quarantined (Inactive) status (unable to make or receive calls) until manually removed from quarantine.</td>
</tr>
<tr>
<td><strong>Apply to VBP</strong></td>
<td>If this option is selected, video border proxies (VBPs) can be blacklisted. If a VBP is blacklisted, none of the endpoints behind it can register.</td>
</tr>
</tbody>
</table>
| **Remove non-hyperactive endpoints from blacklist after specified interval (minutes)** | The interval for which an endpoint must be well-behaved (that is, not exceed the blacklisting threshold for the specified interval) in order to be removed from the blacklist and once again allowed to register. When an endpoint is removed from the blacklist, the Call Server:  
  • Starts interpreting, responding to, auditing, and logging messages of that type from the endpoint.  
  • Clears the alert and SNMP trap.  
  • Logs the removal from the blacklist.  
  **Note:** If the endpoint was quarantined as well as blacklisted, it remains quarantined. |

3. Click **Update** to save the settings.
Dial Plans

Dial plans control how the RealPresence DMA system’s call server uses dial strings to determine where to route calls. You can associate different dial plans for individual call services such as H.323, SIP, or WebRTC. You can also associate specific dial plans to calls received from guest ports.

This flexibility allows you to assign different dial plans to separate SIP servers, neighbored gatekeepers, or session border controllers within your video conferencing environment.

The system comes with two dial plans out-of-the-box: a default dial plan and a guest dial plan. The Default Dial Plan provides the most commonly needed address resolution processing and is used for authorized calls. The Guest Dial Plan is used for unauthorized “guest” calls and contains no dial rules. The Guest Dial Plan blocks all guest calls unless you add dial rules to it to allow unauthorized calls.

You can add additional dial plans as needed. You can also add, edit, remove, and change the order of the dial rules that are included in the default dial plan. Dial strings may match multiple dial rules, but the rules have a priority order. When the RealPresence DMA system receives a call request and associated dial string, it applies the first matched (highest priority) dial rule within the associated dial plan.

You can test a dial plan using the Test Dial Plan action. You can specify various caller parameters and a dial string, and see how the selected dial rules handle such a call. See Default Dial Plan and Suggestions for Modifying the Default Dial Plan.

Dial Rules

Dial rules specify how the RealPresence DMA system Call Server uses a dial string to determine where to route a call. The dial string may include an IP address, a string of numbers that begin with a prefix associated with a service, a string that begins with a country code and city code, or a string that matches a particular alias for a device.

Dial strings may match multiple dial rules, but the rules have a priority order. When the RealPresence DMA system Call Server receives a call request and associated dial string, it applies the first matched (highest priority) dial rule.

A dial rule consists of an optional preliminary script to modify dial strings and the action to be performed, which you select from a defined list of actions. The actions apply dial resolution logic.

For example, the Resolve to registered endpoint action applies all the associated system configurations and performs various searches on the internal endpoint registration records to determine if the inbound call is attempting to reach another registered endpoint. It automatically adjusts for signaling protocol, case, and standard dial string deviations to locate a registered endpoint. You do not have to account for these variables in your dial plan because the logic behind the dial rule action does so for you.
# Default Dial Plan

The Polycom RealPresence DMA system is configured by default with a generic dial plan that covers many common call scenarios. The following table describes the default dial plan:

<table>
<thead>
<tr>
<th>Default Rule Description</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  Dial registered endpoints by alias</td>
<td>If the dial string is the alias or SIP URI of a registered endpoint, the call is routed to that endpoint.</td>
</tr>
<tr>
<td>2  Dial by conference room ID</td>
<td>Otherwise, if the dial string is the dial-in number of a conference room on the Polycom RealPresence DMA system, the call is routed to that conference room.</td>
</tr>
<tr>
<td>3  Dial to SIP conference factory</td>
<td>Otherwise, if the dial string is the dial-in number of a SIP conference factory, the call is routed to that SIP conference factory.</td>
</tr>
<tr>
<td>4  Dial by virtual entry queue ID</td>
<td>Otherwise, if the dial string is the dial-in number of a virtual entry queue on the Polycom RealPresence DMA system, the call is routed to that VEQ.</td>
</tr>
<tr>
<td>5  Dial to on-premises RealConnect™ conference</td>
<td>Otherwise, if the dial string is the dial-in number of a Skype for Business conference on the Skype AVMCU, the call is routed to an available Polycom MCU that supports Skype for Business and is automatically connected to the corresponding Skype conference on the AVMCU. (If no Polycom MCUs that support Skype for Business are available, the conference fails to start). <strong>Note:</strong> This rule is disabled by default.</td>
</tr>
<tr>
<td>6  Dial services by prefix</td>
<td>Otherwise, if the dial string begins with the configured prefix of a service (such as an MCU, ISDN gateway, SBC, neighbor gatekeeper, SIP peer proxy, or simplified ISDN dialing service) the call is routed to that service. <strong>Note:</strong> For a SIP peer, the dial string must either include the protocol or consist of only the prefix and user name (no @domain). For instance, if the SIP peer’s prefix is 123, the dial string for a call to <a href="mailto:alice@polycom.com">alice@polycom.com</a> must be one of the following: sip:<a href="mailto:123alice@polycom.com">123alice@polycom.com</a> 123alice</td>
</tr>
<tr>
<td>7  Dial external networks by H.323 URL, Email ID, or SIP URI</td>
<td>Otherwise, if the address is an external address, the call is routed to that external address. H.323 and SIP calls use the designated SBC for the originating site to reach addresses outside the enterprise network. Examples of external addresses: ;<a href="mailto:johnsmith@someothercompany.com">johnsmith@someothercompany.com</a> sip:<a href="mailto:johnsmith@someothercompany.com">johnsmith@someothercompany.com</a></td>
</tr>
</tbody>
</table>
Suggestions for Modifying the Default Dial Plan

If you have special configuration needs and want to modify the default dial plan, be aware that some of the default dial rules are necessary for “normal” operation. Removing or modifying them takes the system out of compliance with ITU and IEEE standards.

Consider the following suggestions and guidelines if you modify the dial plan:

- Polycom recommends ordering dial rules so that the rule with the action Resolve to external SIP peer appears last in the list. If a dial rule with the action Resolve to external SIP peer doesn’t successfully route a call, the call is aborted and no subsequent dial rules will be attempted. Polycom also recommends that this rule not appear higher than its default order in the list of dial rules, because this can prevent valid aliases, VMRs, and VEQs from being dialed and can result in reduced system performance.

- To add an MCU, ISDN gateway, SBC, neighbor gatekeeper, SIP peer, or simplified dialing service that can be dialed by prefix, configure the prefix range of the new service on the appropriate page. No dial plan change is necessary, since the rule Dial services by prefix of the default dial plan takes care of dialing by prefix.

- You can remove or disable a default dial rule if you don't want the associated functionality. Note that the rule Dial endpoints by IP address is used in several scenarios where calls are received from neighbor gatekeepers or SBCs. Removing it breaks these scenarios.

- If certain dial strings are matching on the wrong dial rule, you may need to re-order the rules.

- In some circumstances (depending on the dial plan and the network topology and configuration), dial rules using the Resolve to external address action or the Resolve to IP address action can enable dialing loops to develop, especially if servers reference each other either directly or via DNS. Common ways to avoid dialing loops include:
  - Use domain restrictions to ensure that the RealPresence DMA system and its peers are each responsible for specific domains.
  - Use a preliminary script like the sample script “SUBSTITUTE DOMAIN (SIP)” (see Sample Preliminary and Postliminary Scripts) to change the domain of a SIP URI dial string to something that will not create a dialing loop.

---

### Default Rule Description

<table>
<thead>
<tr>
<th>Default Rule Description</th>
<th>Effect</th>
</tr>
</thead>
</table>
| **8** Dial endpoints by IP address | Otherwise, if the address is an IP address, the call is routed to that IP address (H.323 calls use the designated SBC for the originating site to reach addresses outside the enterprise network). Examples of IP addresses:  
  - 1.2.3.4  
  - 1.2.3.4##abc  
  - sip:abc@1.2.3.4  
  - sip:1.2.3.4@mycompany.com |
| **9** Dial to RealConnect™ conference by external Lync system conference ID | Otherwise, if the dial string is the dial-in number of a Lync or Skype conference on an external Lync or Skype system, the call is routed to an available Polycom MCU that supports RealConnect™ conferences for external Lync or Skype systems. (If no Polycom MCUs that support RealConnect™ conferences for external Lync or Skype systems are available, the conference fails to start).  
  **Note**: This rule is disabled by default, but is required if any external Lync or Skype systems are defined. |
Use a postliminary script to similarly change the domain before sending to a peer.

Use configuration options on the peers to prevent loops.

Create a dial rule that uses the Block action and a preliminary script to enhance the system's ability to prevent dialing loops for specific types of calls. The preliminary script ensures that the dial rule only matches the types of calls you want to block. This dial rule should be ordered after other dial rules that are expected to resolve the intended call requests.

For example, a dial rule with the Block action using the following preliminary script blocks all call requests that use a prefix of "44" if they have not been resolved by previous dial rules:

```
println("DIAL_STRING=" + DIAL_STRING);
var prefix='44'
var re = RegExp('^(sip:|sips:|h323:|tel:)?'+ prefix +'.*'')
if(! DIAL_STRING.match(re))
{
    println("NEXT_RULE");
    return NEXT_RULE;
}
println("ACCEPT and terminate 44 prefix calls if they were not resolved by previous dial rules");
```

- You can add a filtering preliminary script to any dial rule to restrict the behavior of that rule.
  For example, if you know that all the aliases of a specific neighbor gatekeeper are exactly ten digits long, you may want to route calls to that gatekeeper only if the dial string begins with a certain prefix followed by exactly ten digits.
  To accomplish this, add a preliminary script to the service prefix dial rule that rejects all dial strings that begin with the prefix, but aren't followed by exactly ten digits.

- To exclude certain dial strings, combine a filtering preliminary script with the Block action.

- You can use a preliminary script to modify the dial strings accepted by any of the rules.
  For example, to be able to call an enterprise partner by dialing the prefix 7 followed by an alias in the partner’s namespace, configure a Resolve to external at transforms the string 7xxxx to xxxx@enterprisepartner.com.

  This type of dial string modification is also useful if you are using Skype for Business conference dial strings with prefixes. To route a dial string with a prefix to a Skype conference ID, configure a Resolve to Skype conference ID action with a preliminary script that removes the prefix from the dial string (1234567 would become 4567, for example).

- If your enterprise includes another gatekeeper and you want to route calls to that gatekeeper without a prefix, add a dial rule using the Resolve to external gatekeeper action.

- If your enterprise includes a SIP peer and you want to route calls to that peer without a prefix, add a dial rule using the Resolve to external SIP peer action.

  If you have multiple SIP peers, a call matching the rule is routed to the first one to answer. You may want to specify the domain(s) for which each is responsible.

  When routing to a SIP peer, the Polycom RealPresence DMA system gives up its ability to route the call to other locations if the peer rejects the call. Consequently, a dial rule using the Resolve to external SIP peer action should generally be the last rule in the dial plan.
In a mixed H.323 and SIP environment, the Polycom RealPresence DMA system acts as a seamless gateway. If an H.323 device sends it a Location Request (LRQ) and the dial plan contains a dial rule using the Resolve to external SIP peer action, the RealPresence DMA system will respond with a Location Confirm (LCF) because it can resolve the address by routing the H.323 call through its gateway to the SIP peer(s). You can prevent H.323 calls from being routed to SIP peers by restricting which calls are routed to them in one or more of the following ways:

- Assign each SIP peer an authorized domain or domains (this is a good idea in any case in order to avoid dialing loops).
- Assign each SIP peer a prefix or prefix range.
- Add a preliminary script to the dial rule using the Resolve to external SIP peer action that ensures that the rule will only match a SIP address.
- Make the dial rule using the Resolve to external SIP peer action the last rule and ensure that all H.323 calls will match against one of the preceding dial rules.

Add a Dial Plan

You can create a new dial plan to be associated with one or more call services such as H.323, SIP or WebRTC. After you create the dial plan, you need to add dial rules and prioritize them.

To add a dial plan:

1. Go to Service Config > Dial Plan > Dial Plans and click Add Dial Plan.
2. Enter a Dial plan name and click OK.

Add a Dial Rule to a Dial Plan

You can add a dial rule to a dial plan and prioritize the dial rule. When the RealPresence DMA system receives a call request and associated dial string, it applies the first matched (highest priority) dial rule within the associated dial plan.

To add a dial rule to a dial plan:

1. Go to Service Config > Dial Plan > Dial Plans.
2. Select the dial plan to which you want to add a rule and click Add Dial Rule.
3. Select Enabled.
   - If this check box is cleared, the dial rule is turned off but remains in the dial plan.
4. Enter a detailed Description of the rule.
5. Select the Action the rule will perform.
The following table describes the **Action** options and how the system attempts to resolve the destination address (dial string) for each action.

<table>
<thead>
<tr>
<th>For this action</th>
<th>The system attempts to resolve the address as follows:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block</td>
<td>Blocks the call.</td>
</tr>
</tbody>
</table>
| Resolve to IP address        | Attempts to treat the dial string as an IP address, and if it can, assumes it's the address (and port, if included) of an unregistered endpoint. If no port is specified, it uses the default port of the signaling protocol. If the dial string contains the characters "##," it tries to do this using the characters before "##." For **SIP:**

  - If the host part is an IP address:
    - If it belongs to one of the systems in the supercluster, the system examines the user part.
    - If it belongs to a local domain, the dial string is resolved unchanged.
    - If it belongs to neither of the above, the dial string is resolved unchanged.
  - If the host part is a hostname or domain:
    - If it belongs to one of the systems in the supercluster, the system examines the user part.
    - If it belongs to a local domain, the system examines the user part.
    - If it belongs to neither of the above, the dial string is passed to the next dial rule.
  - When the system examines the user part, it takes one of the following actions:
    - If the user part is an IP address, it resolves the call to that IP address. For example, the dial string `sip:1.2.3.4@10.1.1.1` would be resolved to `sip:1.2.3.4`.
    - If the user part contains "##" and the preceding characters are an IP address, the characters after "##" are treated as the user part of a URI. For example, if the user part has the format `ip-addr##string`, the system resolves the call to the dial string `sip:string@ip-addr`.
  - The user part examination fails (and the dial string is passed to the next dial rule) if the user part isn't in one of the following formats:
    - IP address
    - IP address##
    - IP address##string

For **H.323**, if the characters before the first "##" resolve to an IP address, the characters after that are converted into the destinationInfo (ACF) or destinationAddress (Setup) as follows:

  - If possible, encoded as a dialedDigits address.
  - Otherwise, if possible, encoded as a url-ID.
  - Otherwise, encoded as an h323-ID.
<table>
<thead>
<tr>
<th>For this action:</th>
<th>The system attempts to resolve the address as follows:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resolve to service prefix</td>
<td>Looks for a service prefix that matches the beginning of the dial string (not counting the URI scheme, if present).</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For a SIP peer, the dial string must either include the protocol or consist of only the prefix and user name (no @domain). For instance, if the SIP peer’s prefix is 123, the dial string for a call to <a href="mailto:alice@polycom.com">alice@polycom.com</a> must be one of the following: sip:<a href="mailto:123alice@polycom.com">123alice@polycom.com</a> 123alice</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Resolve to conference ID by Skype query</th>
<th>Queries an integrated Skype SIP peer for a Skype AV/MCU-based conference with a matching conference ID. This dial rule action enables Polycom RealConnect™ functionality for Skype on-premise systems only; it does not apply to external Skype systems. When selected, the following fields are available:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <strong>Conference template</strong></td>
</tr>
<tr>
<td></td>
<td>When checked, you can select the conference template used to start the conference. If you leave this option unchanged, the Default conference template configured in <strong>Admin &gt; Conference Manager &gt; Conference Settings</strong> will be used. Keep in mind that the conference template must specify a Conference mode of AVC only, or the conference will not start.</td>
</tr>
<tr>
<td></td>
<td>• <strong>MCU pool order</strong></td>
</tr>
<tr>
<td></td>
<td>When checked, select the MCU pool order to use for MCUs that provide Skype AV/MCU cascade functionality.</td>
</tr>
<tr>
<td></td>
<td>When the dial rule initiates a new Polycom RealConnect™ conference, one of the selected external SIP peers resolves the conference ID. The RealPresence DMA system then uses the MCU pool order configured for the external SIP peer that hosts the conference to select an MCU. If no MCU pool order is configured for the external SIP peer that hosts the conference, the dial rule uses the MCU pool order you select in this field to route the conference to an MCU. If you leave this option unchecked, the dial rule will use the default pool order selected in the Default MCU pool order field on the <strong>Admin &gt; Conference Manager &gt; Conference Settings</strong> page.</td>
</tr>
<tr>
<td></td>
<td>• <strong>MCU Affinity</strong></td>
</tr>
<tr>
<td></td>
<td>When checked, you can select the MCU Affinity as follows:</td>
</tr>
<tr>
<td></td>
<td>▲ <strong>Prefer MCU in first MCU pool</strong></td>
</tr>
<tr>
<td></td>
<td>The RealPresence DMA system routes the call to the first available MCU in the first MCU pool. If no MCU is available, the system searches the second MCU pool for an available MCU, and so on. This setting is recommended to help ensure that the MCU selected is optimal based on its geographic proximity to the Skype AV/MCU.</td>
</tr>
<tr>
<td></td>
<td>▲ <strong>Prefer MCU in first caller’s site</strong></td>
</tr>
<tr>
<td></td>
<td>Matches the MCU chosen for the call with the site that the first caller’s endpoint belongs to.</td>
</tr>
<tr>
<td></td>
<td>When not checked, defaults to the value in the <strong>MCU Selection</strong> field on the Admin &gt; Conference Manager &gt; Conference Settings page.</td>
</tr>
</tbody>
</table>
### Dial Plans

<table>
<thead>
<tr>
<th>For this action:</th>
<th>The system attempts to resolve the address as follows:</th>
</tr>
</thead>
</table>
| Resolve to Skype Conference ID by Conference Auto Attendant | Examines the beginning of the dial string, searching for the longest matching prefix of a defined external Skype system. If a match is found, the dial rule removes the prefix from the dial string and passes the resulting conference ID to the Polycom MCU, which then contacts the CAA of the matched external Skype system.  
If an external Skype system is listed on the Integrations > External Skype Systems page, it is available in the Available external Skype systems box. You can move external Skype systems to which the rule applies to the Selected external Skype systems box.  
A dial rule with this action is required for Polycom MCUs to connect to Skype conferences on external Skype systems. |
| Resolve to external SIP peer | Checks the domain of the dial string against all of the rule’s selected peers, looking for a peer proxy responsible for that domain. If the dial string matches the domain of one of the selected SIP peers, this rule will either successfully route the call, or the call will be aborted; no subsequent dial rules are attempted.  
After selecting this action for a rule, select a Routing policy. The policy affects the way the system resolves dial strings to SIP peers:  
• **All in parallel (forking)**  
The system uses all SIP peers simultaneously to try to resolve the dial string.  
• **Weighted round-robin**  
You can assign each SIP peer a weight in the range 1-100, with a higher weight giving a SIP peer higher priority; the system tries each SIP peer sequentially according to the SIP peer’s assigned weight. You can assign a SIP peer different weights in different dial rules.  
After choosing a routing policy, move the SIP peers to which the rule applies from the Available SIP peers box to the Selected SIP peers box. If the Weighted round-robin routing policy is selected, choose a weight for the selected SIP peer using the Edit weight button.  
**Note:** This action employs the H.323<->SIP gateway function if applicable. |
| Resolve to external gatekeeper | If the dial string appears to be an H.323 alias, simultaneously sends LRQ messages to all of the rule’s selected gatekeepers.  
After selecting this action for a rule, move the gatekeepers to which the rule applies from the Available gatekeepers box to the Selected gatekeepers box.  
**Note:** This action employs the H.323<->SIP gateway function if applicable. |
**Dial Plans**

In the **Preliminary** tab, add a preliminary script. A preliminary is an executable script, written in the Javascript language, that defines processing actions (filtering or transformation) that are part of a dial rule and may be applied to a dial string before the dial rule's action is performed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Resolve to external address** | Determines if the dial string is a well-formed instance of an external address type to which the rule applies, and if so, uses the resolution procedures specified in the applicable standard for that address type. After selecting this action for a rule, select the address type or types to which the rule applies. The address types and applicable standards used to resolve them are:  
  - SIP URI: RFCs 3261 and 3263  
  - H.323 url-ID: H.323 specification, Annex O  
  - H.323 Email-ID: H.225.0 specification, Appendix IV |
| **Resolve to registered endpoint** | Looks for a registered endpoint (active or inactive) that has the same alias or signaling address.  
**Note:** This action employs the H.323<>SIP gateway function if applicable. |
| **Resolve to conference room** | Looks for a conference room (virtual meeting room, or VMR) that matches the dial string. |
| **Resolve to SIP conference factory** | Determines if the dial string contains a SIP conference factory ID and, if so, creates a multi-point conference on an MCU and generates a conference ID for the conference. The conference IDs are strings that can be dialed by any endpoint (SIP or H.323) to join the conference. |
| **Resolve to virtual entry queue** | Looks for a shared-number entry queue that matches the dial string. |

6. In the **Preliminary** tab, add a preliminary script. A preliminary is an executable script, written in the Javascript language, that defines processing actions (filtering or transformation) that are part of a dial rule and may be applied to a dial string before the dial rule's action is performed.

7. Select the **Enabled** check box.

8. Type (or paste) the preliminary script you want to apply.

   **Sample Preliminary and Postliminary Scripts** provides examples you can experiment with and modify for your purposes.

9. Click **Debug this Script** to open the **Script Debugging** window.

10. Specify the parameters of a call and the dial string, and assess what effect the script has on the dial string:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Dial string**        | The DIAL_STRING variable in the script, which is initially set to the dial string being evaluated. Enter a dial string to test. Alternatively, provide the entire SIP INVITE message. Then click **Execute Script**.  
**Note:** For SIP, the script should always specify the schema prefix (sip or sips). For instance:  
DIAL_STRING = "sip:xxx@10.33.120.58" |
| **Caller site**        | Select a site to set the first four caller variables. |
| **Caller variables**   | Lists variables that can be used in the script to represent caller alias values. Enter an alias value to test for that variable. |
### Edit a Dial Rule

You can edit a dial rule within a dial plan. You can update the preliminary script or the action used, or you can disable the rule.

**To edit a dial rule:**

1. Go to **Service Config > Dial Plan > Dial Plans**.
2. Select the dial plan to which the dial rule belongs.
3. Select the rule you want to edit and click **Edit Dial Rule**.
4. Revise the fields as described in the following table as needed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Dial Rule</strong></td>
<td></td>
</tr>
<tr>
<td>Enabled</td>
<td>Clearing this check box lets you turn off a rule without deleting it.</td>
</tr>
<tr>
<td>Description</td>
<td>The text description displayed on the Dial Rules page.</td>
</tr>
<tr>
<td>Action</td>
<td>The action to be performed. When you select some actions, additional settings become available.</td>
</tr>
<tr>
<td></td>
<td>See the table of dial rule actions below for more information about the actions and the additional settings associated with them.</td>
</tr>
<tr>
<td>Preliminary</td>
<td>A preliminary is an executable script, written in the Javascript language, that defines processing actions (filtering or transformation) that are part of a dial rule and may be applied to a dial string before the dial rule’s action is performed.</td>
</tr>
<tr>
<td></td>
<td><strong>Sample Preliminary and Postliminary Scripts</strong> provides some examples you can experiment with and modify for your purposes.</td>
</tr>
</tbody>
</table>

11 Click **Execute Script** to test your preliminary script.
Associating a Dial Plan to a Call Service

You can associate a dial plan with each call service you have enabled for your call server. You can also assign a dial plan for both authorized and unauthorized (guest port) calls.

See Signaling Settings.

**Associate a Dial Plan to SIP Service**

In SIP Settings, you can select a dial plan to associate with both unencrypted and TLS ports.

To associate a dial plan with a SIP call service:

1. Go to Service Config > SIP Settings.
2. Under Authorized ports, use the Dial plan drop-down list to select a dial plan for both the Unencrypted SIP port and TLS port.
3. Click Update to save your settings.

**Associate a Dial Plan to H.323 Service**

In H.323 Settings, you can select a dial plan to associate with

To associate a dial plan with H.323 call service:

1. Go to Service Config > H.323 Settings.
2. Select the Dial plan to apply to H.323 calls.
3. Click Update to save your settings.

**Associate a Dial Plan to WebRTC Service**

In WebRTC Settings, you can select a dial plan for both authorized and unauthorized WebRTC calls.

To associate a dial plan with WebRTC call service:

1. Go to Service Config > WebRTC Settings.
2. Select the Authorized Dial plan and Unauthorized Dial plan to apply to WebRTC calls.
3. Click Update to save your settings.
**Test a Dial Plan**

You can specify various caller parameters and a dial string, and see how the each dial rule handles such a call and what its final disposition is.

**To test a dial plan:**

1. Go to **Service Config > Dial Plan > Dial Plans**.
2. In the **Dial Plan** list, select a dial plan to test and click **Test Dial Plan**.
3. Complete the fields in the following table as required.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dial string</td>
<td>Enter a dial string to test. Then click <strong>Test</strong>. For SIP, the dial string should always specify the schema prefix (sip or sips). For example: <code>sips:rbruce@10.47.7.9</code></td>
</tr>
<tr>
<td>Caller site</td>
<td>Select a site in order to set the four caller site variables: • CALLER_SITE_NAME • CALLER_SITE_DIGITS • CALLER_SITE_COUNTRY_CODE • CALLER_SITE_AREA_CODE These variables can’t be set directly and are display only.</td>
</tr>
<tr>
<td>CALLER_H323ID</td>
<td>Test caller’s H323-ID or blank.</td>
</tr>
<tr>
<td>CALLER_E164</td>
<td>Test caller’s H.323 E.164 alias or blank.</td>
</tr>
<tr>
<td>CALLER_TEL_URI</td>
<td>Test caller’s SIP tel URI or blank.</td>
</tr>
<tr>
<td>CALLER_SIP_URI</td>
<td>Test caller’s SIP sip URI or blank.</td>
</tr>
<tr>
<td>VMR/Skype Conf ID</td>
<td>This field specifies the return value of the function <code>getConferenceRoomOrID()</code>*, and is only populated when the dial rule simulates an outbound call to an endpoint from a conference based on a VMR or Skype conference ID. If the dial rule simulates a call to a VMR or Skype conference ID or a dial-in call, this field is blank.</td>
</tr>
</tbody>
</table>
Complete the required fields and click Test.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Test route output   | Displays the results of applying each rule (including its preliminary, if any) to the dial string. For instance, testing the dial string example shown above against the default dial plan might result in the following:  
  #1: SipAlias[sips:rbruce@10.47.7.9] is not registered. H323-ID[rbruce] is not registered.  
  #2: The room [rbruce] does not exist.  
  #3: No entry queue is found.  
  #4: Domain [10.47.7.9] is not within our administration.  
  #5: The call was accepted by this dial rule. |
| Final result        | Displays the final outcome of the dial rule processing. The final outcome for the example above would be:  
  Transformed dial string is [sips:rbruce@10.47.7.9]. The call was accepted by dial rule #5. |
Prefix Service

The Prefix Service list provides all configured prefixes in one place so you can determine what prefixes are in use and whether any conflicts exist. You can perform the following actions on a service or device with a prefix:

- Add, edit, or delete any of the devices without having to navigate back to the specific page for that device type. Devices include an external gatekeeper, external SIP peer, external H.323 SBC, and MCU.
- Add, edit, or delete simplified ISDN gateway dialing services.
- Edit the name, vertical service code, or description of the forwarding and hunt group services and enable or disable them.

The following table describes the fields in the list.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service/Device Name</td>
<td>The name of the service or device assigned the specified prefix(es). Devices with no prefix(es) assigned are listed, but shown as disabled.</td>
</tr>
<tr>
<td>Prefix Range</td>
<td>The dial string prefix(es) assigned to this service or device.</td>
</tr>
<tr>
<td>Service/Device Type</td>
<td>Type of service or device.</td>
</tr>
<tr>
<td>Description</td>
<td>Brief description of the service or device.</td>
</tr>
<tr>
<td>Service Status</td>
<td>Indicates whether the service or device is enabled or disabled.</td>
</tr>
</tbody>
</table>

Add Simplified ISDN Gateway Dialing Prefix

You can create a new prefix-driven simplified ISDN gateway dialing service for using external ISDN gateways.

This feature is not related to the Polycom RealPresence DMA system’s built-in H.323<->SIP gateway. Simplified ISDN gateway dialing is for routing calls to H.320 or PSTN protocol gateways.

This feature is not supported for calls from SIP endpoints, but SIP endpoints can make ISDN gateway calls by directly calling an MCU/gateway using its direct dial-in prefix (see Edit an MCU).

To add a simplified ISDN gateway dialing prefix:

1. Go to Service Config > Dial Plan > Prefix Service.
2. Click Add Simplified ISDN Gateway Dialing.
3 Complete the fields in the following table as required.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A display name for this service.</td>
</tr>
<tr>
<td>Description</td>
<td>Brief description of the service.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Clearing this check box lets you turn off the service without deleting it.</td>
</tr>
<tr>
<td>Simplified ISDN dialing prefix</td>
<td>The dial string prefix(es) assigned to this service.</td>
</tr>
<tr>
<td></td>
<td>Enter a single prefix (44), a range of prefixes (44-47), multiple prefixes</td>
</tr>
<tr>
<td></td>
<td>separated by commas (44,46), or a combination (41, 44-47, 49).</td>
</tr>
<tr>
<td></td>
<td>If your dial plan uses the Dial services by prefix dial rule (in the default dial plan) to route calls to services, all dial strings beginning with an assigned prefix are forwarded to this service for resolution.</td>
</tr>
<tr>
<td>Use all ISDN gateways</td>
<td>Indicates whether this service applies to all available gateways or only those selected below.</td>
</tr>
<tr>
<td>Available ISDN gateways</td>
<td>Lists the ISDN gateways that have at least one session profile specifying an H.320 or PSTN protocol. See Edit an MCU.</td>
</tr>
<tr>
<td>Selected ISDN gateways</td>
<td>Lists the selected ISDN gateways. The arrow buttons move gateways from one list to the other.</td>
</tr>
</tbody>
</table>

4 Click OK.

**Edit Simplified ISDN Gateway Dialing Prefix**

You can edit a prefix-driven simplified ISDN gateway dialing service.

This feature is not related to the Polycom RealPresence DMA system's built-in H.323<->SIP gateway. Simplified ISDN gateway dialing is for routing calls to H.320 or PSTN protocol gateways. This feature isn’t supported for calls from SIP endpoints, but SIP endpoints can make ISDN gateway calls by directly calling an MCU/gateway using its direct dial-in prefix.

**To edit a simplified ISDN gateway dialing prefix:**

1 Go to Service Config > Dial Plan > Prefix Service.
2 Select a Simplified ISDN Gateway Dialing service and click Edit.
3 Revise the fields in the following table as required:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A display name for this service.</td>
</tr>
<tr>
<td>Description</td>
<td>Brief description of the service.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Clearing this check box lets you turn off the service without deleting it.</td>
</tr>
</tbody>
</table>
Prefix Service

You can edit a call forwarding or hunt group service invoked when callers dial the vertical service code (VSC) for that service, followed by the alias. These services are included on the Prefix Service page and cannot be deleted, but you can disable them or change their names, descriptions, or VSCs. If you change the VSCs, be sure to inform users of the change.

To edit a vertical service code:

1. Go to Service Config > Dial Plan > Prefix Service.
2. Select a service or device with a vertical service code.
3. Click Edit.
4. Revise the fields in the following table as required:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simplified ISDN dialing prefix</td>
<td>The dial string prefix(es) assigned to this service. Enter a single prefix (44), a range of prefixes (44-47), multiple prefixes separated by commas (44,46), or a combination (41, 44-47, 49). If your dial plan uses the Dial services by prefix dial rule (in the default dial plan) to route calls to services, all dial strings beginning with an assigned prefix are forwarded to this service for resolution.</td>
</tr>
<tr>
<td>Use all ISDN gateways</td>
<td>Indicates whether this service applies to all available gateways or only those selected below.</td>
</tr>
<tr>
<td>Available ISDN gateways</td>
<td>Lists the gateways that have at least one session profile specifying an H.320 or PSTN protocol.</td>
</tr>
<tr>
<td>Selected ISDN gateways</td>
<td>Lists the selected gateways. The arrow buttons move gateways from one list to the other.</td>
</tr>
</tbody>
</table>

4. Click OK.

Edit Vertical Service Code

You can edit a call forwarding or hunt group service invoked when callers dial the vertical service code (VSC) for that service, followed by the alias. These services are included on the Prefix Service page and cannot be deleted, but you can disable them or change their names, descriptions, or VSCs. If you change the VSCs, be sure to inform users of the change.

To edit a vertical service code:

1. Go to Service Config > Dial Plan > Prefix Service.
2. Select a service or device with a vertical service code.
3. Click Edit.
4. Revise the fields in the following table as required:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The type of service. This field cannot be edited.</td>
</tr>
<tr>
<td>Name</td>
<td>A display name for this service.</td>
</tr>
<tr>
<td>Code</td>
<td>The vertical service code (VSC) for this service. Must consist of an asterisk/star (*) followed by two digits. Registered endpoints can activate this feature by dialing the VSC followed by the alias. They can deactivate it by dialing the VSC alone.</td>
</tr>
<tr>
<td>Description</td>
<td>Brief description of the service.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Clearing this check box turns off the service.</td>
</tr>
</tbody>
</table>

5. Click OK.
Hunt Groups

A hunt group is a set of endpoints that share an alias or aliases. Hunt groups can be used to define a dial string shared by a group of people, such as a technical support number. When the Polycom RealPresence DMA system Call Server resolves a dial string to the hunt group’s alias, it selects a member of the group and tries to terminate the call to that member.

The system selects hunt group members in round-robin fashion. It skips members that are in a call or have unconditional call forwarding enabled. If the selected group member rejects the call or doesn’t answer before the timeout, the system tries the next group member.

If all members have been attempted (or skipped) without successfully terminating the call, the system sends the BUSY message to the caller.

Registered endpoints can add themselves to a hunt group by dialing the vertical service code (VSC) for joining (default is *71) followed by the hunt group alias. They can leave a hunt group by dialing the VSC for leaving (default is *72) followed by the hunt group alias. An endpoint can belong to multiple hunt groups.

The Hunt Groups page lists the defined hunt groups and lets you add, edit, and delete hunt groups. The following table describes the fields in the list.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Hunt group name.</td>
</tr>
<tr>
<td>Description</td>
<td>Brief description of the hunt group.</td>
</tr>
<tr>
<td>Aliases</td>
<td>The aliases (dial strings) that resolve to this hunt group.</td>
</tr>
<tr>
<td>Members</td>
<td>The endpoints included in the hunt group.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Indicates whether the hunt group is being used.</td>
</tr>
</tbody>
</table>

Add a Hunt Group

You can define a new hunt group in the system and add members to it.

To add a hunt group:

1. Go to Service Config > Dial Plan > Hunt Groups.
2. In the Actions list click Add.
   
   The Add Hunt Group dialog appears displays the following fields.
Complete the required fields and click OK.

**Edit a Hunt Group**

You can modify the selected hunt group and add or remove members.

**To edit a Hunt Group:**

1. Go to Service Config > Dial Plan > Hunt Groups.
2. Select the hunt group of interest and click Add.

   The **Edit Hunt Group** dialog displays the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Info</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Hunt group name.</td>
</tr>
<tr>
<td>Description</td>
<td>The text description displayed in the <strong>Hunt Groups</strong> list.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Clearing this check box lets you stop using a hunt group without deleting it.</td>
</tr>
<tr>
<td>No answer timeout</td>
<td>Number of seconds to wait for a hunt group member to answer a call before giving up and trying another member.</td>
</tr>
<tr>
<td>Aliases</td>
<td>Lists the aliases (dial strings) that resolve to this hunt group. Click <strong>Add</strong> to add an alias. Click <strong>Edit</strong> or <strong>Delete</strong> to change or remove the selected alias.</td>
</tr>
</tbody>
</table>

---

**Hunt Group Members**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search</td>
<td>Search for endpoints by alias, IP address, or registration status.</td>
</tr>
<tr>
<td>Available endpoints</td>
<td>Lists the endpoints that match the search criteria.</td>
</tr>
<tr>
<td>Member endpoints</td>
<td>Lists the endpoints to include in the hunt group. Use the arrow buttons to move endpoints from one list to the other.</td>
</tr>
</tbody>
</table>

3. Complete the required fields and click **OK**.
Complete the required fields and click OK.

Add an Alias
- Add an Alias
- Edit an Alias

Add an Alias
You can add an alias value to the hunt group.

To add an alias:
1. Go to Service Config > Dial Plan > Hunt Groups.
2. In the Actions list click Add.
   - The Add Hunt Group dialog appears.
3. Under the Alias Type list, click Add.
   - Aliases should be specified by their fully qualified dial string. For example, to specify that H.323 callers can call the hunt group by dialing 1234, enter 1234. To specify that SIP callers can call the hunt group by dialing 1234, enter sip:1234@mydomain.com.
4. Fill in the Value field in the Add Alias dialog and click OK.

Edit an Alias
You can change an alias value assigned to the hunt group.

To edit an alias:
1. Go to Service Config > Dial Plan > Hunt Groups.
2. In the Actions list click Edit.
   - The Edit Hunt Group dialog appears.
3. Under the Alias Type list, click Edit.
   - Aliases should be specified by their fully qualified dial string. For example, to specify that H.323 callers can call the hunt group by dialing 1234, enter 1234. To specify that SIP callers can call the hunt group by dialing 1234, enter sip:1234@mydomain.com.
4. Fill in the Value field in the Edit Alias dialog and click OK.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hunt Group Members</td>
<td></td>
</tr>
<tr>
<td>Search</td>
<td>Search for endpoints by alias, IP address, or registration status.</td>
</tr>
<tr>
<td>Available endpoints</td>
<td>Lists the endpoints that match the search criteria.</td>
</tr>
<tr>
<td>Member endpoints</td>
<td>Lists the endpoints to include in the hunt group. Use the arrow buttons to move endpoints from one list to the other.</td>
</tr>
</tbody>
</table>
Domains Restrictions

On the Domain Restrictions page, you can add administrative domains to or remove them from the list of domains from which registrations are accepted.

If the list is empty, all domains are considered local, and the system accepts endpoint registrations from any domain. Otherwise, it accepts registrations only from the listed domains. This is a supercluster-wide configuration.

Calls that have a non-local domain in the dialed string do not resolve to any locally registered endpoints, and can only resolve to a VEQ or VMR if the Conference rooms belong to every domain check box is checked.

Note: The Resolve to external address dial rule action does not match against domains that are considered local. If the list of domains is empty and all domains are considered local, this dial rule action won’t match any dial string and can’t be used.

In some circumstances (depending on network topology and configuration), dialing loops can develop if you don’t restrict the RealPresence DMA system to specific domains.

Add a Local Domain

You can add a local domain to the system.

To add a local domain:

1. Go to Service Config > Dial Plan > Domain Restrictions.
2. In the Add new local domain field, enter a domain and click Add.
   
   IP addresses (including IP addresses with the wildcard character) and domain names are accepted.

Remove a Local Domain

You can remove a local domain from the system.

To remove a local domain:

1. Select a domain from the Local domains list and click Remove.
2. Click Restore Defaults to remove all domains so that the system accepts registrations from any domain.
### Domain Restrictions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add new local domain</td>
<td>Enter a domain and click Add to add it to the Local domains list. IP addresses (including IP addresses with the wildcard character) and domain names are accepted. Domain names must be valid and full domains, but you can replace a single host label within a domain with the wildcard character to match multiple subdomains. For instance, <em>.mycompany.com matches: eng.mycompany.com fin.mycompany.com And eng.</em>.mycompany.com matches: eng.sanjose.mycompany.com eng.austin.mycompany.com Subdomains are not local if the domain is listed without a wildcard character. For example, if the domain mycompany.com is entered without any other mycompany domains, this would NOT match eng.mycompany.com.</td>
</tr>
<tr>
<td>Local domains</td>
<td>The list of domains from which the system accepts registrations. Select a domain and click Remove to remove it from the list. Click Restore Defaults to remove all domains so that the system accepts registrations from any domain.</td>
</tr>
<tr>
<td>Locally registered SIP endpoints belong to every local domain</td>
<td>Specifies that call requests for locally registered SIP endpoints don’t have to match the domain. For example, if there is an endpoint registered as sip:johnsmith@1.1.1.1 and this option is enabled, a call to sip:<a href="mailto:johnsmith@mycompany.com">johnsmith@mycompany.com</a> may be connected to that endpoint. If this option is not selected, call requests must exactly match the URI of the registered endpoint.</td>
</tr>
<tr>
<td>Email IDs of registered H.323 endpoints belong to every local domain</td>
<td>Specifies that call requests for locally registered H.323 endpoints’ email IDs don’t have to match the domain. For example, if there is an endpoint registered as johnsmith@1.1.1.1 and this option is enabled, a call to <a href="mailto:johnsmith@mycompany.com">johnsmith@mycompany.com</a> may be connected to that endpoint. If this option is not selected, call requests must exactly match the URI of the registered endpoint.</td>
</tr>
<tr>
<td>Conference rooms and virtual entry queues belong to every domain</td>
<td>Specifies that if the dial string specifies a conference room (VMR) or virtual entry queue (VEQ) on the Polycom RealPresence DMA system and includes a domain, a dial rule implementing the Resolve to conference room ID or Resolve to virtual entry queue actions (such as dial rule #2 or #3 of the default dial plan) ignores the domain and routes the call to that conference room or VEQ. If this option is not selected, a dial string’s domain must be a local domain for the system to route the call to a conference room or VEQ.</td>
</tr>
</tbody>
</table>
Preliminary and Postliminary Scripting

A preliminary is an executable script, written in the Javascript language, that defines processing actions (filtering or transformation) to be applied to a dial string before the dial rule’s action is performed.

A postliminary is an executable script, written in the Javascript language, that defines dial string transformations to be applied before querying an external device (gatekeeper, SIP peer, SBC, or MCU).

Transformation scripts output some modification of the DIAL_STRING variable (which is initially set to the dial string being evaluated).

Filtering scripts may pass the dial string on to the dial rule’s action (if the filter criteria aren’t met) or return one of the following:

- NEXT_RULE: Skips the rule being processed and passes the dial string to the next rule.
- BLOCK: Rejects the call.

See Sample Preliminary and Postliminary Scripts for script examples.

Predefined Preliminary/Postliminary Scripting Variables

The following table describes the predefined variables you can use in a preliminary or postliminary script. The script can evaluate a variable or change its value (the change isn’t preserved after the script completes).

<table>
<thead>
<tr>
<th>Variable</th>
<th>Initial value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CALLER_E164</td>
<td>For H.323 calls only, an array variable initially set to the set of E.164 addresses of the caller. The length of the array is 0 if the caller doesn’t have an E.164 address.</td>
</tr>
<tr>
<td>CALLER_H323ID</td>
<td>Array variable initially set to the set of H323ID addresses of the caller. The length of the array is 0 if the caller doesn’t have an H323ID address.</td>
</tr>
<tr>
<td>CALLER_IS_IPV6</td>
<td>“TRUE” if the caller is an IPv6 endpoint. Blank otherwise.</td>
</tr>
<tr>
<td>CALLER_SIP_URI</td>
<td>Array variable initially set to the set of SIP URI addresses of the caller. The length of the array is 0 if the caller doesn’t have a SIP URI address.</td>
</tr>
<tr>
<td>CALLER_SITE_AREA_CODE</td>
<td>Area code of the caller’s site. Blank if the site doesn’t have an area code.</td>
</tr>
<tr>
<td>CALLER_SITE_COUNTRY_CODE</td>
<td>Country code of the caller’s site. Blank if the site doesn’t have a country code.</td>
</tr>
<tr>
<td>CALLER_SITE_DIGITS</td>
<td>The number of subscriber number digits in the caller’s site (that is, the length of a phone number at the site, excluding area code). Blank if the site doesn’t have a number of digits.</td>
</tr>
<tr>
<td>Variable</td>
<td>Initial value</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>CALLER_SITE_NAME</td>
<td>The name of the caller’s site.</td>
</tr>
<tr>
<td>CALLER_TEL_URI</td>
<td>Array variable initially set to the set of Tel URI addresses of the caller. The length of the array is 0 if the caller doesn’t have a Tel URI address.</td>
</tr>
<tr>
<td>DIAL_STRING</td>
<td>Initially set to the dial string being evaluated. If the script modifies the DIAL_STRING value, the modified value is used as the input to the dial rule action. For SIP, when the DIAL_STRING is modified by the script, it’s use depends on the dial rule action:</td>
</tr>
<tr>
<td>INPUT_SIP_HEADERS</td>
<td>For SIP calls only, an associative array containing the SIP headers in the received SIP INVITE message.</td>
</tr>
<tr>
<td></td>
<td>Usage example:</td>
</tr>
<tr>
<td></td>
<td>if(INPUT_SIP_HEADERS[&quot;Supported&quot;]).matches(/.<em>ms-forking.</em>))/</td>
</tr>
<tr>
<td></td>
<td>{</td>
</tr>
<tr>
<td></td>
<td>...</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td>OUTPUT_SIP_HEADERS</td>
<td>An empty associative array. Headers that the script adds to this array replace the corresponding headers in the received SIP INVITE message. If a header added to this array isn’t in the received INVITE message, it’s added to the INVITE message.</td>
</tr>
<tr>
<td></td>
<td>Usage example 1:</td>
</tr>
<tr>
<td></td>
<td>var list = OUTPUT_SIP_HEADERS.get(&quot;User-Agent&quot;);</td>
</tr>
<tr>
<td></td>
<td>if (list == null)</td>
</tr>
<tr>
<td></td>
<td>{</td>
</tr>
<tr>
<td></td>
<td>list = new java.util.LinkedList();</td>
</tr>
<tr>
<td></td>
<td>OUTPUT_SIP_HEADERS.put(&quot;User-Agent&quot;, list);</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>list.add(&quot;Someone. Not a RealPresence DMA 7000.&quot;);</td>
</tr>
<tr>
<td></td>
<td>Usage example 2:</td>
</tr>
<tr>
<td></td>
<td>var list = OUTPUT_SIP_HEADERS.get(&quot;Some-Custom-Header&quot;);</td>
</tr>
<tr>
<td></td>
<td>if (list == null)</td>
</tr>
<tr>
<td></td>
<td>{</td>
</tr>
<tr>
<td></td>
<td>list = new java.util.LinkedList();</td>
</tr>
<tr>
<td></td>
<td>OUTPUT_SIP_HEADERS.put(&quot;Some-Custom-Header&quot;, list);</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>list.add(&quot;Whatever you want&quot;);</td>
</tr>
</tbody>
</table>
Preliminary/Postliminary Scripting Functions

The following table describes the functions you can use in a preliminary or postliminary script. The parentheses at the end of the function name contain the parameters, if any, that the function accepts.

<table>
<thead>
<tr>
<th>Function name and parameters</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>getConferenceRoomOrID()</td>
<td><strong>Return value:</strong>&lt;br&gt;• For dial-outs to endpoints from VMRs or Polycom RealConnect™ conferences, returns the VMR or Skype Conference ID.&lt;br&gt;• For dial-outs to the VMR or Polycom RealConnect™ conferences, and for dial-ins, returns the empty string.</td>
</tr>
<tr>
<td>getHeader(&lt;SIP header name&gt;)</td>
<td><strong>Return value:</strong> Returns the contents of the specified SIP header in the original SIP INVITE request.&lt;br&gt;<strong>Note:</strong> The return value is not changed if the SIP header is changed with setHeader.</td>
</tr>
<tr>
<td>setHeader(&lt;SIP header name&gt;, &lt;text&gt;)</td>
<td>Replaces the current contents of the specified SIP header in the output version of the SIP INVITE request with &lt;text&gt;.&lt;br&gt;<strong>Return value:</strong> None.&lt;br&gt;<strong>Note:</strong> Any changes made using setHeader do not affect subsequent values returned by getHeader.</td>
</tr>
<tr>
<td>getDisplayName(&lt;text&gt;)</td>
<td><strong>Return value:</strong> Returns the display name portion of &lt;text&gt;.&lt;br&gt;<strong>Note:</strong> This function assumes that &lt;text&gt; uses the format of a SIP INVITE “To” header.</td>
</tr>
<tr>
<td>getUser(&lt;text&gt;)</td>
<td><strong>Return value:</strong> Returns the user portion of &lt;text&gt;.&lt;br&gt;<strong>Note:</strong> This function assumes that &lt;text&gt; uses the format of a SIP INVITE “To” header.</td>
</tr>
<tr>
<td>getParameterString(&lt;text&gt;)</td>
<td><strong>Return value:</strong> Returns the parameter string portion of &lt;text&gt;.&lt;br&gt;<strong>Note:</strong> This function assumes that &lt;text&gt; uses the format of a SIP INVITE “To” header.</td>
</tr>
<tr>
<td>appendParameterString(&lt;header Text&gt;, &lt;text&gt;)</td>
<td><strong>Return value:</strong> Returns the result of appending &lt;text&gt; to the end of &lt;headerText&gt;, using the format of a SIP INVITE “To” header.</td>
</tr>
<tr>
<td>removeHeader(&lt;text&gt;)</td>
<td>Removes the header named &lt;text&gt; from the SIP INVITE.&lt;br&gt;<strong>Return value:</strong> None.</td>
</tr>
<tr>
<td>getPeerHost()</td>
<td><strong>Return value:</strong>&lt;br&gt;• If invoked from an External SIP Peer postliminary script, returns the Next hop address configured for this SIP peer.&lt;br&gt;• Otherwise, returns the empty string.</td>
</tr>
</tbody>
</table>
How Dial Rule Actions Affect SIP Headers

The following table shows how different dial rule actions apply a preliminary script’s modified dial string to the output SIP headers in a SIP call.

<table>
<thead>
<tr>
<th>Dial rule action</th>
<th>Output SIP headers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resolve to registered endpoint</td>
<td>The To header is replaced with the modified dial string. The request URI is based on the contact address of the registered endpoint, and not replaced with the modified dial string.</td>
</tr>
<tr>
<td>Resolve to external address</td>
<td>The To header and the request URI are both replaced with the modified dial string.</td>
</tr>
</tbody>
</table>
| Resolve to service prefix         | For a SIP peer proxy of type OCS:  
The To header is replaced with the modified dial string. The request URI is based on the address, port, and transport type of the proxy, and not replaced with the modified dial string.  
For a SIP peer proxy of type Other:  
The To header and the request URI are both replaced with the modified dial string. |

Function name and parameters | Details |
|-----------------------------|---------|
| getPeerNetOrNextHop()       | Return value:  
• If invoked from an External SIP Peer postliminary script, returns one of the following:  
  ▲ The Destination network value configured for this SIP peer, if defined  
  ▲ The Next hop address for this SIP peer, if the Destination network setting is not configured  
• If not invoked from an External SIP Peer postliminary script, returns the empty string. |

getPeerPort() | Return value:  
• If invoked from an External SIP Peer postliminary script, returns the IP network Port configured for this SIP peer.  
• Otherwise, returns the empty string. |

getPeerTransport() | Return value:  
• If invoked from an External SIP Peer postliminary script, returns the Transport type configured for this SIP peer.  
• Otherwise, returns the empty string. |
To test preliminary and postliminary scripts:

1. Go to **Service Config > Dial Plans**.
2. Select a dial plan.
3. Select the dial rule with the script to test and click **Edit Dial Rule**.
4. On the **Preliminary** tab, select **Debug this Script**.
5. Complete the script debugging details as described in the following table:

<table>
<thead>
<tr>
<th><strong>Field</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
</table>
| Dial string               | This is the DIAL_STRING variable in the script, which is initially set to the dial string being evaluated. Enter a dial string to test. Alternatively, provide the entire SIP INVITE message. Then click **Execute Script**.  
  **Note:** For SIP, the script should always specify the schema prefix (sip or sips).  
  For instance:
  
  DIAL_STRING = "sip:xxx@10.33.120.58" |
| Caller site               | Select a site in order to set the first four caller variables.                   |
| Caller variables          | Lists variables that can be used in the script to represent caller alias values. Enter an alias value to test for that variable. |
| VMR/transient conf ID     | This field specifies the return value of the function getConferenceRoomOrID().  
  If the script simulates a call to a VMR or transient conference ID or a dial-in call, this field is blank. |
| Final result              | Displays the outcome of running the script.  
  For a dial rule preliminary, if the script rejected the dial string (skipping the dial rule action and passing it on to the next dial rule), a message tells you so. Otherwise, the transformed dial string is displayed. |
Preliminary and Postliminary Scripting

Sample Preliminary and Postliminary Scripts

A preliminary is an executable script, written in the Javascript language, that defines processing actions (filtering or transformation) to be applied to a dial string before the dial rule’s action is performed.

A postliminary is an executable script, written in the Javascript language, that defines dial string transformations to be applied before querying an external device (gatekeeper, SIP peer, SBC, or MCU).

Transformation scripts output some modification of the DIAL_STRING variable (which is initially set to the dial string being evaluated).

Filtering scripts may pass the dial string on to the dial rule’s action (if the filter criteria aren’t met) or return one of the following:

- NEXT_RULE: Skips the rule being processed and passes the dial string to the next rule.
- BLOCK: Rejects the call.

The following sample scripts address many of the scenarios for which you might need a preliminary or postliminary script. You can use them as templates or starting points for your scripts.

```
// Example preliminary and postliminary scripts

////////////////////////////////////
// STRIP PREFIX
// If the dial string has prefix 99, remove it
// 991234 --> 1234
DIAL_STRING = DIAL_STRING.replace(/^99/,"");

////////////////////////////////////
// ADD PREFIX
// Add prefix 99 to the dial string
// 1234 --> 991234
DIAL_STRING = "99" + DIAL_STRING;

////////////////////////////////////
// STRIP PREFIX (SIP)
// If the dial string is a SIP URI with prefix 99 in the user part, remove it
// SIP:991234@abc.com --> sip:1234@abc.com
```

6 Click **Execute Script** to test the preliminary script.
DIAL_STRING = DIAL_STRING.replace(/sip:99\([^@]*@)/i,"sip:$1");

////////////////////////////////////////////////////
// ADD PREFIX (SIP)
// If the dial string is a SIP URI, add prefix 99 to the user part
// SIP:1234@abc.com  -->  sip:991234@abc.com
DIAL_STRING = DIAL_STRING.replace(/sip:(\[^@]*@)/i,"sip:99$1");

////////////////////////////////////////////////////
// SUBSTITUTE DOMAIN (SIP)
// If the dial string is a SIP URI, change the domain part to "example.com"
// SIP:1234@abc.com  -->  sip:1234@example.com
DIAL_STRING = DIAL_STRING.replace(/sip:(\[^@]*)@(.*)/i,"sip:$1@example.com");

////////////////////////////////////////////////////
// FILTER
// If the dial string has prefix 99, do not match on this rule. Skip to the next rule.
// 991234  -->  NEXT_RULE
if (DIAL_STRING.match(/^99/))
{  
  return NEXT_RULE;
}

////////////////////////////////////////////////////
// FILTER (Inverted)
// Do not match on this rule unless the dial string has prefix 99.
// 1234  -->  NEXT_RULE
if (!DIAL_STRING.match(/^99/))
{  
  return NEXT_RULE;
}

////////////////////////////////////////////////////
// FILTER (SIP)
// If the dial string is a SIP URI with domain "example.com", do not match on this rule.
// Skip to the next rule.
// sip:1234@example.com  -->  NEXT_RULE
if (DIAL_STRING.toLowerCase().match(/^sip:\[^@]*@example\.com/))
{  
  return NEXT_RULE;
}
// Preliminary and Postliminary Scripting

// PRINTLN
// Print out the information available to the script for this call.
// Information printed using the print or println functions
// is saved as a call audit event, which is viewable in the
// DMA interface under Reports > Call History, and also in the
// Script Debugging dialog box.

println("DIAL_STRING: " + DIAL_STRING);
println("CALLER_SITE_NAME: " + CALLER_SITE_NAME);
println("CALLER_SITE_COUNTRY_CODE: " + CALLER_SITE_COUNTRY_CODE);
println("CALLER_SITE_AREA_CODE: " + CALLER_SITE_AREA_CODE);
println("CALLER_SITE_DIGITS: " + CALLER_SITE_DIGITS);
println("CALLER_H323ID: " + CALLER_H323ID);
println("CALLER_E164: " + CALLER_E164);
println("CALLER_TEL_URI: " + CALLER_TEL_URI);
println("CALLER_SIP_URI: " + CALLER_SIP_URI);

// FILTER (Site)
// Do not allow callers from the atlanta site to use this rule.
// (Caller site == "atlanta")  -->  NEXT_RULE

if (CALLER_SITE_NAME == "atlanta")
{
    return NEXT_RULE;
}

// SITE BASED NUMERIC NICKNAMES
// Allow caller to omit country and area code when calling locally.
// Assumes that country and area codes are set in site topology.
// Assumes that all endpoints are registered with their full alias, including
// country and area code.
// 5551212  --> 14045551212

if (DIAL_STRING.length == CALLER_SITE_DIGITS)
{
    DIAL_STRING = CALLER_SITE_COUNTRY_CODE + CALLER_SITE_AREA_CODE + DIAL_STRING;
}
else if (DIAL_STRING.length == (parseInt(CALLER_SITE_AREA_CODE.length,10)
    + parseInt(CALLER_SITE_DIGITS,10)))

    DIAL_STRING = CALLER_SITE_COUNTRY_CODE + DIAL_STRING;
}
SITE BASED NUMERIC NICKNAMES (SIP)

Allow caller to omit country and area code when calling locally.
Assumes that country and area codes are set in site topology.
Assumes that all endpoints are registered with their full alias, including
country and area code.

sip:5551212@example.com  --> sip:14045551212@example.com

```javascript
if (DIAL_STRING.toLowerCase().match(/sip:[^@]*@example.com/))
{
    user = DIAL_STRING.replace(/sip:(^@)*@.*/i,"$1");
    if (user.length == CALLER_SITE_DIGITS)
    {
        user = CALLER_SITE_COUNTRY_CODE + CALLER_SITE_AREA_CODE + user;
    }
    else if (user.length == (parseInt(CALLER_SITE_AREA_CODE.length,10)
+ parseInt(CALLER_SITE_DIGITS,10)))
    {
        user = CALLER_SITE_COUNTRY_CODE + user;
    }
    DIAL_STRING = "sip:" + user + "@example.com";
}
```

LIMITING CALLS TO A CERTAIN NUMERIC DIAL RANGE.

(like the range specified Conference Settings screen)

```javascript
var minGeneratedRoomId = 1000;
var maxGeneratedRoomId = 9999;
var number  = parseInt(DIAL_STRING.replace(/sip:(^@)*@?.*/i,"$1"));

if (isNaN(number) || number > minGeneratedRoomId && number < maxGeneratedRoomId)
{
    return;
}
return NEXT_RULE;
```

A sample script that routes all dial-out calls from a
whitelist of VMRs to a SIP peer with prefix 11. All other dial-out
calls will be routed to a SIP peer with prefix 22.
The getConferenceRoomOrID() function returns a value only when
the call is a dial-out from a VMR or Skype scheduled conference
to an endpoint.

```javascript
var whitelist_vmrs = [
```
"1000", // Specify list of VMRs; add or remove VMRs from this list.
"2000", // Make sure you use the syntax "<vmr number>"
"3000",
];
var prefix = "22";

////////////////////////////////
// Match against individual VMRs. ACCEPT if any of them matches.
//
if (0 <= whitelist_vmrs.indexOf(getConferenceRoomOrID()))
{
    prefix = "11";
}
DIAL_STRING = prefix + DIAL_STRING;

////////////////////////////////
// This script may be useful with "Resolve to external SIP peer" dial rules.
//
// This script skips this dial rule unless the call is SIP or SIPS. (Without
// this, the H.323-SIP gateway function could be invoked).

if (!DIAL_STRING.match(/sips?:/i))
{
    return NEXT_RULE;
}

////////////////////////////////
// This script may be useful with "Resolve to registered endpoint" dial rules.
//
// This script applies to registered H.323 endpoints calling registered SIP
// endpoints (e.g., 1001, 1002, ...) and forces a H.323-SIP gateway call by
// adding the "sip:" dialing scheme.
//
// System configuration: Replace sip.domain.com with your system's SIP domain.

DIAL_STRING = DIAL_STRING.replace(/(^1001$)/,"sip:$1@sip.domain.com");
DIAL_STRING = DIAL_STRING.replace(/(^1002$)/,"sip:$1@sip.domain.com");

////////////////////////////////
// This script may be useful with "Resolve to registered endpoint" dial rules.
//
// This script applies to registered SIP endpoints calling registered H.323
// endpoints (e.g., 1001, 1002, ...) and forces a SIP-H.323 gateway call by
// removing the dialing scheme.
//
// System configuration: Replace sip.domain.com with your system's SIP domain.
Preliminary and Postliminary Scripting

DIAL_STRING = DIAL_STRING.replace(/sips?:\(1001\)@sip.domain.com.*,"$1");
DIAL_STRING = DIAL_STRING.replace(/sips?:\(1002\)@sip.domain.com.*,"$1");

////////////////////////////////////////////
// This script illustrates how to accept SIP dial strings that include upper case
// characters and convert them into dial strings with only lower case characters. Thus,
// calls to sip:AbCdEfG123@MyDomain.com are converted to sip:abcdefg123@mydomain.com.
//
// This script can configured as the preliminary for a dial rule with the action "Resolve
// to registered endpoint".
//
// CAUTION: This script should be used in conjunction with some method to assure that all
// SIP registered endpoints have only lower-case characters. One way to assure this is to
// use this script in conjunction with a registration policy script that only allows
// endpoints with lower case SIP URIs to register. See "Sample Preliminary and
// Postliminary Scripts."
//
// Applying this script to other dial rules can cause problems with interoperability.
// For example, if this script is applied to calls to external SIP peers, then the
// endpoints that are eventually contacted through those SIP peers must have lower case
// SIP URIs, or the calls will fail.
//
// Convert all SIP dial strings to lower case and record instances where the dial string
// was changed.
//
// if (CALLER_SIP_URI != null && CALLER_SIP_URI != "") {
    var origDS = DIAL_STRING;
    DIAL_STRING = DIAL_STRING.toLowerCase();
    if (origDS != DIAL_STRING) {
        println("Dial string case changed. Original dialstring=" + origDS + " Lowered=" +
DIAL_STRING);
    }
}

////////////////////////////////////////////
// This script may be useful with "Resolve to registered endpoint" or "Resolve
// to conference room ID" dial rules.
//
// This script prepends a prefix (8237) to any 4 digit dial string beginning
// with 4, 5, or 6 (SIP or H.323).
DIAL_STRING=DIAL_STRING.replace(/^[4-6]\[0-9\]{3}$/,"8237$1");
DIAL_STRING=DIAL_STRING.replace(/^(sips?:)[4-6]\[0-9\]{3}$/,"$18237$2");
DIAL_STRING=DIAL_STRING.replace(/^(sips?:)[4-6]\[0-9\]{3}@/,"$18237$2");

////////////////////////////////////////////
// This script may be useful with "Resolve to service prefix" dial rules.
//
// This applies to PSTN or ISDN dial-outs from H.323 endpoints where the E.164
// number is prefixed with 9.
// The MCU is configured with prefix 2082 and 001 is the gateway session
// prefix. The MCU expects ** as the delimiter for the E.164 number.

DIAL_STRING=DIAL_STRING.replace(/^9([0-9]*)$/,"2082001**$1");

////////////////////////////////
// This script may be useful with "Resolve to external gatekeeper" dial rules
// that send h323 calls to a Cisco VCS device.
//
// This script skips this dial rule if the call is SIP or SIPs. (Without this,
// the SIP-H.323 gateway function would be invoked).
// For H.323 Annex O dial strings of the form <alias>@<domain>, this script
// prepends the dialing scheme "h323:".

if (DIAL_STRING.match(/^sips?:/i))
{
    return NEXT_RULE;
}
else
{
    DIAL_STRING=DIAL_STRING.replace(/(^sips?:)([^@]*)@.*/i,"h323:$1$2");
    println("new dial string is: " + DIAL_STRING);
}

////////////////////////////////
// This script may be useful with "Resolve to external SIP peer" dial rules.
// System configuration: Each SIP peer selected in the dial rule is configured
// with a prefix (11, 22, or 33).
// The script skips this dial rule for dial strings that are'nt SIP, whose alias
// isn't 5 characters, or that don't specify one of the prefixes.
// For dial strings that meet these criteria, the domain is removed.

alias = DIAL_STRING.replace(/sips?:([^@]*@.*/i,"$1");
if (alias.length != 5)
{
    return NEXT_RULE;
}
if (alias.match(/^11/) || alias.match(/^22/) || alias.match(/^33/))
{
    DIAL_STRING = DIAL_STRING.replace(/(^sips?:)([^@]*@.*/i,"$1$2");
    println("new DIAL STRING: " + DIAL_STRING);
}
else


```java
{
    return NEXT_RULE;
}

///////////////////////////////
// This script may be useful with various dial rules.
//
// This script skips this dial rule if the dial string is not a 10 digit
// number. This works for both H.323 and SIP.

alias = DIAL_STRING.replace(/sips?:(\[^@]*).*/i,"$1");
if (!alias.match(/^[0-9]{10}$/))
{
    return NEXT_RULE;
}

///////////////////////////////
// This script may be useful with "Resolve to conference room ID" dial rules.
//
// If there are conference rooms with the same numbers as registered endpoints,
// this script adds a prefix for conference rooms to distinguish them.

if(CALLER_SITE_NAME.match(/USDMAs/))
{
    if(!(DIAL_STRING.match(/^[^61^61]^61|^(sip:61|h323:61)/))){
        if(DIAL_STRING.match(/^sip:/))
        {
            DIAL_STRING = DIAL_STRING.replace(/^sip:(\[^@]*@)/i,"sip:61$1");
        }
        else if(DIAL_STRING.match(/^h323:/))
        {
            DIAL_STRING = DIAL_STRING.replace(/^h323:(\[^@]*@)/i,"h323:61$1");
        }
        else
        {
            DIAL_STRING = "61" + DIAL_STRING;
        }
        println("New translated DIAL_STRING: "+DIAL_STRING);
    }
    if(!(DIAL_STRING.match(/^[^61^61]^61|^(sip:61|h323:61)/))){
        return NEXT_RULE;
    }
}
```

---

Polycom, Inc. 297
Access Control

This section provides an introduction to configuring access control for the Polycom® RealPresence® DMA® system. It includes:

- Registration Policy
- Device Authentication
In the RealPresence DMA system, you can specify policies to control registration by endpoints. The following policies can be defined:

- **Compliance policy**: Includes an executable script (using the Javascript language) that specifies the criteria for determining whether an endpoint is compliant or noncompliant with the registration policy.

- **Admission policy**: Specifies the action to be taken when an endpoint is compliant, and the action to be taken when an endpoint is non-compliant. You can choose from the following actions:
  - **Accept registration** — The endpoint’s registration request is accepted and its status becomes Active (see Endpoints for more information about endpoint status values).
  - **Block registration** — The endpoint’s registration request is rejected and its status becomes Blocked. The system automatically rejects registration attempts (and unregistration attempts) from blocked endpoints without applying the registration policy. The status remains unchanged until you manually unblock the endpoints.
  - **Reject registration** — The endpoint’s registration request is rejected and its status remains not registered. It doesn’t appear in the Endpoints list. Whether it can make and receive calls depends on the system’s rogue call policy (see Call Server Settings). If the endpoint sends another registration request, the system applies the registration policy to that request.
  - **Quarantine registration** — The endpoint’s registration request is accepted, but its status becomes Quarantined. It cannot make or receive calls. The system processes registration attempts (and unregistration attempts) from quarantined endpoints, but does not apply the registration policy. An endpoint’s status remains either Quarantined if registered or Quarantined (Inactive) if unregistered until you manually remove it from quarantine.

### Registration Policy Scripting

A registration policy script is an executable script, written in the Javascript language, that defines the criteria to be applied to registration requests in order to determine what to do with them. The script can specify various criteria and can be as broad or narrow as you want.

A script can return **COMPLIANT** or **NONCOMPLIANT**. The corresponding settings on the Registration Policy page let you specify what action to take for each of these return values.

A script can also assign a value (up to 1000 characters) to the **EP EXCEPTION** variable. This variable’s initial value is blank (empty string). Assigning a non-blank value to it causes an exception to be recorded for the endpoint being processed. Exceptions appear on the Endpoints page, and you can search for endpoints with exceptions.

Exceptions can serve a variety of purposes, from specifying the reason a registration was rejected to simply recording information about the request for future reference. For instance, you may want all endpoints to conform to a specific alias dial string pattern, but not want to quarantine those that do not comply. Assigning an exception to non-compliant endpoints allows you to find them on the Endpoints page so that you can contact the owners.
See Sample Preliminary and Postliminary Scripts for some script examples.

**Registration Policy Script Predefined Variables**

The following table describes the predefined variables you can use in a registration policy script. Each time the script runs, it gets the initial values for these variables from the registration request being processed. The script can evaluate a variable or change its value (the change isn’t preserved after the script completes).

<table>
<thead>
<tr>
<th>Variable</th>
<th>Initial value</th>
</tr>
</thead>
<tbody>
<tr>
<td>EP_DEFINED_IN_CMA</td>
<td>“TRUE” if the Polycom RealPresence DMA system is integrated with a RealPresence Resource Manager system and the endpoint is defined in that system.</td>
</tr>
<tr>
<td>EP_H323_DIALEDDIGITS_ALIAS</td>
<td>Endpoint alias value associated with H.323 dialedDigits or blank. This is an array that can contain multiple values. Separate the values with commas.</td>
</tr>
<tr>
<td>EP_H323_EMAIL_ID_ALIAS</td>
<td>Endpoint alias value associated with H.323 email-ID or blank. This is an array that can contain multiple values. Separate the values with commas.</td>
</tr>
<tr>
<td>EP_H323_H323_ID_ALIAS</td>
<td>Endpoint alias value associated with H.323 H323-ID or blank. This is an array that can contain multiple values. Separate the values with commas.</td>
</tr>
<tr>
<td>EP_H323_TRANSPORT_ID_ALIAS</td>
<td>Endpoint alias value associated with H.323 transportID or blank. This is an array that can contain multiple values. Separate the values with commas.</td>
</tr>
<tr>
<td>EP_H323_URL_ID_ALIAS</td>
<td>Endpoint alias value associated with H.323 URL-ID or blank. This is an array that can contain multiple values. Separate the values with commas.</td>
</tr>
<tr>
<td>EP_IP</td>
<td>Endpoint IP address. Enter it here in normal dot or colon notation (such as 1.2.3.4 for IPv4). In the script, this is represented as an array. If the IP address is IPv4, there are 4 elements in the array. If the IP address is IPv6, there are 8 elements in the array.</td>
</tr>
<tr>
<td>EP_IS_IPV4</td>
<td>“TRUE” if EP_IP is an IPv4 address. Blank otherwise.</td>
</tr>
<tr>
<td>EP_MODEL</td>
<td>Endpoint model.</td>
</tr>
<tr>
<td>EP_OWNER</td>
<td>Endpoint owner.</td>
</tr>
<tr>
<td>EP_OWNER_DOMAIN</td>
<td>Endpoint owner's domain.</td>
</tr>
<tr>
<td>EP_REG_IS_H323</td>
<td>“TRUE” if the registration request uses H.323 signaling. Blank otherwise.</td>
</tr>
</tbody>
</table>
### Variable | Initial value
--- | ---
EP_REG_IS_SIP | “TRUE” if the registration request uses SIP signaling. Blank otherwise.
EP_SIP_SIP_URI_ALIAS | Endpoint alias value associated with SIP sip: URI or blank. This is an array that can contain multiple values. Separate the values with commas.
EP_SIP_SIPS_URI_ALIAS | Endpoint alias value associated with SIP SIPS: URI or blank. This is an array that can contain multiple values. Separate the values with commas.
EP_SIP_TEL_URI_ALIAS | Endpoint alias value associated with SIP TEL: URI or blank. This is an array that can contain multiple values. Separate the values with commas.
EP_VERSION | Endpoint software version number.
REG_IS_PERMANENT | “TRUE” if endpoint is already permanently registered. Blank otherwise.
REG_SITE_AREA_CODE | Area code of the site where the endpoint is attempting to register.
REG_SITE_COUNTRY_CODE | Country code of the site where the endpoint is attempting to register.
REG_SITE_DIGITS | Number of digits in the subscriber number configured for the site where the endpoint is attempting to register.
REG_SITE_NAME | Site where endpoint is attempting to register.
REG_SUBNET_IP_ADDRESS | IP address of the subnet where the endpoint is attempting to register. Enter it here in normal dot or colon notation (such as 1.2.3.4 for IPv4). In the script, this is represented as an array. If the IP address is IPv4, there are 4 elements in the array. If the IP address is IPv6, there are 8 elements in the array.
REG_SUBNET_MASK | IP mask of the subnet where the endpoint is attempting to register. Enter it here in normal dot or colon notation (such as 1.2.3.4 for IPv4). In the script, this is represented as an array. If the IP address is IPv4, there are 4 elements in the array. If the IP address is IPv6, there are 8 elements in the array.

## Configure a Registration Policy

You can configure a registration policy to control registration by endpoints. The policy can be applied only to new registrations, or also to re-registrations with changed properties.
To configure a registration policy:

1. Go to Service Config > Access Control > Registration Policy.
2. Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow site-less registrations</td>
<td>When selected, endpoints that don’t belong to a configured site or territory can register with the Call Server. Otherwise, only endpoints in a subnet configured in the site topology can register.</td>
</tr>
<tr>
<td>Inactive registration deletion (days)</td>
<td>Select to specify that endpoints whose status is Inactive (that is, their registrations have expired) are deleted from the system after the specified number of days. Some dial rule actions, such as Resolve to registered endpoint, can route calls to endpoints with an inactive registration. Deleting the registration record is the only way to prevent resolution to an inactive endpoint.</td>
</tr>
<tr>
<td>Policy applies only to new devices</td>
<td>When selected, the system applies the registration policy script only to new devices.</td>
</tr>
<tr>
<td>Policy applies to new or changed devices</td>
<td>When selected, the system applies the registration policy script to new device registrations and also to changed re-registrations. You can optionally select Ignore IP and port changes so that the registration policy script is not applied if those are the only changes.</td>
</tr>
<tr>
<td>When compliant</td>
<td>Select the action to take when the registration policy script returns COMPLIANT.</td>
</tr>
<tr>
<td>When noncompliant</td>
<td>Select the action to take when the registration policy script returns NONCOMPLIANT.</td>
</tr>
<tr>
<td>Registration policy compliance script</td>
<td>Type (or paste) the registration policy script you want to apply. Then click Debug this Script to test the script with various variables. Click Reapply Policy to run the script, applying any changes you’ve made to existing registered endpoints.</td>
</tr>
</tbody>
</table>

3. Click Debug this Script to test the script with various dial strings and other parameters.
4. Click Update.
   - A Javascript parser evaluates the registration policy script. If the script contains a syntax error, an error message reports the problem and asks if you still want to update. You may do so to save a work in progress, but the script won’t be used until it’s valid.

5. Click Apply Policy to activate the policy.

**Debug a Registration Policy Script**

You can test and debug a registration policy script by using test values for the variables used in your script. Testing your script is an iterative process. Repeat as often as necessary to see the results of applying your script using different variable values.

If necessary, make changes to your script and then test some more, until you’re satisfied that the script accomplishes what you intended.
To debug a registration policy script:

1. Go to Service Config > Access Control > Registration Policy and complete the registration policy settings as needed.
2. Type (or paste) the registration policy script you want to apply.
3. Click Debug this Script to display the Script Debugging window.
4. Enter or select test values for the predefined variables.
5. Select an Endpoint Site and Subnet to populate the site/subnet-related fields, which are read-only.
6. Click Execute Script.

The Script Output box displays any output produced by the script when it runs (e.g., println statements and error messages). This output is recorded in the registration history.

The Script Result box displays the return value (COMPLIANT or NONCOMPLIANT) from running the script with the specified test values. If the script assigned a value to the EP_EXCEPTION variable, it displays that value.

Sample Registration Policy Scripts

A registration policy script is an executable script, written in the Javascript language, that defines the criteria to be applied to registration requests in order to determine what to do with them. For each request evaluated, the script must return COMPLIANT or NONCOMPLIANT. See Registration Policy Scripting for more information.

The following sample scripts illustrate some of the ways in which registration requests can be evaluated. You can use them as templates or starting points for your scripts.

```javascript
VAR result = COMPLIANT;

if (EP_VERSION == "1.2.3.4")
{
    EP_EXCEPTION += "Problem version 1.2.3.4 is not allowed\n";
    result = NONCOMPLIANT;
}

if (!EP_REG_IS_H323)
{
    EP_EXCEPTION += "SIP is not allowed\n";
    result = NONCOMPLIANT;
}
return result;
```

```javascript
VAR result = COMPLIANT;

if (EP_VERSION == "1.2.3.4")
{
    EP_EXCEPTION += "Problem version 1.2.3.4 is not allowed\n";
    result = NONCOMPLIANT;
}

if (!EP_REG_IS_H323)
{
    EP_EXCEPTION += "SIP is not allowed\n";
    result = NONCOMPLIANT;
}
return result;
```
var result = COMPLIANT;

    EP_EXCEPTION += "SIPVicious is not allowed."
    result = NONCOMPLIANT;
} return result;

// This script illustrates how to integrate an existing registration policy script,
// such as the detection and blocking of penetration attacks like SIPVicious, with a
// policy that allows only endpoints with lower-case SIP URIs to register, while blocking
// registrations from endpoints whose SIP URIs contain upper case characters.

// The script only detects the conditions and returns "COMPLIANT" or "NONCOMPLIANT"; the
// registration policy can then be configured to block registrations from non-compliant
// endpoints.

// CAUTION: This script should be used in conjunction with a dial rule preliminary script
// that converts SIP dial strings that include upper case characters into dial strings
// with only lower case characters. See "Sample Registration Policy Scripts."

var result = COMPLIANT;
    EP_EXCEPTION += "SIPVicious is not allowed."
    result = NONCOMPLIANT;
} return result;

var epssua = EP_SIP_SIP_URI_ALIAS + EP_SIP_SIPS_URI_ALIAS;
if (EP_REG_IS_SIP && epssua !== epssua.toLowerCase()) {
    result = NONCOMPLIANT;
    EP_EXCEPTION += "Noncompliant SIP Registration: Endpoint URI " + epssua + " contains upper-case letters."
} return result;

// Reject aliases that aren't the right length; otherwise accept.
// IF REG_SITE_COUNTRY_CODE = 1
//   AND IF REG_SITE_AREA_CODE = 303
//   AND IF REG_SITE_DIGITS = 4
// IF EP_H323_DIALEDDIGITS_ALIAS[0].length() != 8
// return NONCOMPLIANT;
var CCAndAC = REG_SITE_COUNTRY_CODE + REG_SITE_AREA_CODE;
var DDlength = EP_H323_DIALEDDIGITS_ALIAS[0].length();
var SumDigits = parseInt(CCAndAC.length) + parseInt(REG_SITE_DIGITS);

if (DDlength > 0)
{
  if (DDlength != SumDigits) return NONCOMPLIANT;
}

/////////////////////////////////////////////////////////////////////
// Reject aliases that don't start with CC and AC (country code and area code); // otherwise accept.
//
var CCAndAC = REG_SITE_COUNTRY_CODE + REG_SITE_AREA_CODE;
var DD_CCAndAC = EP_H323_DIALEDDIGITS_ALIAS[0].substring(0,CCAndAC.length);

if (DD_CCAndAC != CCAndAC) return NONCOMPLIANT;

/////////////////////////////////////////////////////////////////////
// Reject aliases that don't start with AC (area code).
//
var AC = REG_SITE_AREA_CODE;
var DD_AC = EP_H323_DIALEDDIGITS_ALIAS[0].substring(0,AC.length);
var SIP_URI_AC = EP_SIP_TEL_URI_ALIAS.substring(0,AC.length);

if (DD_AC != AC) return NONCOMPLIANT;
if (SIP_URI_AC != AC) return NONCOMPLIANT;

/////////////////////////////////////////////////////////////////////
// A sample script that implements a whitelist of IP addresses for endpoints // that can register.
// *** Note this does not take into account IPv6 addressing ***
//
var nparts;
var IPstring;

whitelist = new Array(
  "10.20.30.40",     // specify exact match IP address using quotes
  /192.168.3.*/,     // specify regular expression to match using slashes
  "192.168.174.233"
);

if (EP_IS_IPV4)
{
  nparts = 4;
}
for (i = 0; i<nparts; i++)
{
    if (i == 0)
    {
        IPstring = EP_IP[i];
    }
    else
    {
        IPstring += "." + EP_IP[i]
    }
}

for (i=0; i<whitelist.length; i++)
{
    if (IPstring.match(whitelist[i]))
    {
        return COMPLIANT;
    }
}
return NONCOMPLIANT;

///////// A sample registration policy script with various combinations of blacklists and whitelists. 
  // Allows white/black listing of endpoints based on IP - Configure the 
  // IPOverride table below. 
  // Allows white/black listing of certain aliases - Configure the 
  // aliasOverride table below. 
  // Allows specific aliases to a given IP - Configure the allowAlias 
  // table below. 
  // An Override Action of "COMPLIANT" whitelists an IP or alias. 
  // An Override Action of "NONCOMPLIANT" blacklists an IP or alias. 
  // Notes: 
  //   IPOverride takes precedence over aliasOverride which takes 
  //   precedence over the IP/Alias associations. 
  // This script only works for IPv4 endpoints. 
  // This script only works for H.323 endpoints that are registering with a single dialed-digits (E.164) alias. 
  // - If it does not have dialed-digits alias or it has multiple 
  //   dialed-digits aliases, the registration is not compliant. 
  // - If it has a single dialed-digits alias AND other aliases, the 
  //   registration is compliant if the dialed-digits alias is in the 
  //   whitelist.
This script only works for SIP endpoints that are registering with a "sip:" URI alias. "sips:" and "tel:" aliases are not supported.

------BEGIN whitelist section------

Enter new lines with the format:
IPOverride["5.6.7.8"] = "Override Action";

var IPOverride = {};
IPOverride["5.6.7.9"] = "COMPLIANT";
IPOverride["8.8.8.8"] = "COMPLIANT";
IPOverride["40.242.225.50"] = "NONCOMPLIANT";

Enter new lines with the format:
aliasOverride["abcd"] = "Override Action";

var aliasOverride = {};
aliasOverride["999"] = "COMPLIANT";
aliasOverride["911"] = "COMPLIANT";
aliasOverride["12345678"] = "NONCOMPLIANT";

Enter new lines with the format:
allowAlias["A.B.C.D"] = "alias or SIP URI";

var allowAlias = {};
allowAlias["10.0.0.15"] = "1234";
allowAlias["172.20.10.5"] = "5678";
allowAlias["192.168.50.1"] = "john.doe@customer.com";

------END whitelist section------

------DO NOT EDIT BELOW THIS LINE------

---Variable definitions---

var IPAlias;
var IPstr = EP_IP[0];
var reg323Alias = EP_H323_DIALEDDIGITS_ALIAS;
var regSipAlias = EP_SIP_SIP_URI_ALIAS.toLowerCase();

---Step 1: EP_IP array is converted into a string for easier use.

for (var i = 1; i < 4; i++){
    IPstr += "." + EP_IP[i];
}

---Step 2: Check the IPOverride hash table to see if we should white/black
// list this IP.

if(IPstr in IPOverride){
    return returnOverride(0,IPstr);
}

//---Step 3: Handle SIP registrations. First, check if the SIP URI is white/black listed.
// If not, check to see if the IP has an allowed alias, and if the URI matches the allowed alias.
// If none of the above, return NONCOMPLIANT.

else if(EP_REG_IS_SIP){
    if(regSipAlias in aliasOverride){
        return returnOverride(1,regSipAlias);
    }
    else if (IPstr in allowAlias){
        sAlias = allowAlias[IPstr];
        return checkAlias(regSipAlias, sAlias);
    }else{
        return NONCOMPLIANT
    }
}

//---Step 4: Handle H.323 registrations. First check if the alias is white/black listed.
// Next, reject registrations with more than 1 alias.
// Then, check if the IP has an allowed alias and check if the provided alias matches.
// If none of the above, return NONCOMPLIANT.

else if(EP_REG_IS_H323){
    if((reg323Alias[0] in aliasOverride) && (typeof(reg323Alias[1])=='undefined')){
        return returnOverride(1,reg323Alias[0]);
    }
    else if(!(typeof(reg323Alias[1])=='undefined')){
        return NONCOMPLIANT;
    }else if (IPstr in allowAlias){
        hAlias = allowAlias[IPstr];
        return checkAlias(reg323Alias[0], hAlias);
    }else{
        return NONCOMPLIANT
    }
}

//---Function definitions---/
//checkAlias function: Compares aliases from a registration and from the white list and returns the appropriate action.

function checkAlias(a0, aWl){
    if(a0 == aWl){
        return COMPLIANT;
    }
    else{
        return NONCOMPLIANT;
    }
}

//returnOverride function: ovrType is 0 (for IP) and 1 (for alias). Checks the ovrVal (IP or Alias) against the appropriate override list and returns the override action.

function returnOverride(ovrType, ovrVal){
    switch (ovrType) {
        case 0:
            return IPOVERRIDE[ovrVal];
            break;
        case 1:
            return aliasOverride[ovrVal];
            break;
    }
}
Device Authentication

Device authentication enhances security by requiring devices registering with or calling the RealPresence DMA system to provide credentials that the system can authenticate. In turn, the RealPresence DMA system may need to authenticate itself to an external SIP peer or gatekeeper.

All authentication configurations are supercluster-wide, but note that the default realm for SIP device authentication is the cluster’s domain as specified in Network Settings. This allows each cluster in a supercluster to have its own realm for challenges.

H.323 Device Authentication

In an environment where H.235 authentication is used, H.323 devices include their credentials (name and password) in registration and signaling (RAS) requests. The RealPresence DMA system authenticates requests as follows:

- If it’s a signaling request (ARQ, BRQ, DRQ) from an unregistered endpoint, the Call Server doesn’t authenticate the credentials.
- Otherwise, if the request is from an endpoint, an MCU, or neighbor gatekeeper, the Call Server attempts to authenticate using its device authentication list.
- If it’s a signaling request from a registered endpoint, or if the request is from an MCU or neighbor gatekeeper, the Call Server attempts to authenticate using its device authentication list.

If the credentials can’t be authenticated, the Call Server rejects the registration or signaling request. For call signaling requests, it also rejects the request if the credentials differ from those with which the device registered.

SIP Device Authentication

When a SIP endpoint registers with or calls the Polycom RealPresence DMA system, if the request includes authentication information, that information is checked against the Call Server’s local device authentication list.

SIP authentication can be enabled at the port/transport level or (for “unauthorized” access prefixes) the prefix level.

If SIP authentication is enabled and an endpoint’s request doesn’t include authentication information, the Call Server responds with an authentication challenge containing the required fields. If the endpoint responds with valid authentication information, the system accepts the registration or call.

Note: If inbound SIP authentication is turned on for a port or prefix, the Polycom RealPresence DMA system challenges any SIP message coming to the system via that port or with that prefix. Any SIP peer and other device that interacts with the system by those means must be configured to authenticate itself, or you must turn off Device authentication for that specific device.
Inbound Authentication

In the Inbound Authentication section, you can configure specific SIP digest authentication settings for SIP devices. You can also maintain the Call Server’s local inbound device authentication list. This list is used for both H.235 authentication (H.323 devices) and SIP digest authentication (SIP devices).

Shared Outbound Authentication

In the Shared Outbound Authentication section, you can maintain the Call Server’s general list of authentication credentials, which it uses to authenticate itself on behalf of calling devices to external SIP peers for which the appropriate device-specific credentials haven’t been defined.

The Call Server intercepts and responds to authentication challenges from SIP peers on behalf of some or all devices calling through the Call Server. This feature allows authentication security between the Call Server and its peers to be completely separate from security between the endpoints and the Call Server.

When you add an external SIP peer, you can specify whether the Call Server handles challenges (401 and 407) on behalf of the source of the call or passes them on to the source of the call. You can also define authentication credentials specifically for that SIP peer.

**Note:** For H.323, when you add a neighbor gatekeeper, you can configure the system to send its H.235 credentials when it sends address resolution requests to that gatekeeper.

The following table describes the fields on the Device Authentication page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound Authentication</td>
<td></td>
</tr>
<tr>
<td>SIP device authentication settings</td>
<td></td>
</tr>
<tr>
<td>Use default realm</td>
<td>This option, the default, sets the realm for the Call Server to the cluster’s domain as specified on the Network Settings page (allowing each cluster of a supercluster to have its own realm). If no domain is specified on the Network Settings page, the default realm value is sip.dma. Clear the check box to change the string in the Realm field.</td>
</tr>
<tr>
<td>Realm</td>
<td>The realm string in an authentication challenge tells the challenged device the protection domain for which it must provide credentials. Generally, it includes the domain label of the Call Server. See RFC 2617 and RFC 3261. If you specify a realm instead of using the default, the realm you specify is used for all clusters in the supercluster.</td>
</tr>
<tr>
<td>Enable proxy authentication</td>
<td>Configures the Call Server to respond to unauthenticated requests with 407 (Proxy Authentication Required). If turned off, the Call Server responds to unauthenticated requests with 401 (Unauthorized).</td>
</tr>
<tr>
<td>Authentication valid time</td>
<td>Specifies the time period within which the Call Server doesn’t re-challenge a device that previously authenticated itself.</td>
</tr>
<tr>
<td>(seconds)</td>
<td></td>
</tr>
</tbody>
</table>
Device Authentication

Add Inbound Device Authentication

You can add a device’s authentication credentials to the list of entries against which the Call Server checks device credentials.

To add a device authentication:

1. Go to Service Config > Access Control > Device Authentication.
2. Click the Add icon.
3. In Add Device Authentication Credentials, complete the fields as described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(table of authentication entries)</td>
<td>Lists the inbound device authentication entries against which the Call Server checks a device’s credentials. Click Add to add a device’s credentials to the list. Click Edit or Delete to change or remove the selected entry.</td>
</tr>
</tbody>
</table>

Shared Outbound Authentication

Lists the authentication credential entries defined for general use by the Call Server to authenticate its requests, showing the realm in which the entry is valid and the user name. You can add, edit, or delete credential entries. Use the Realm or Name field and Search button above the list to narrow the list. When choosing authentication credentials to present to an external SIP peer, the Call Server looks first for an appropriate entry specific to that SIP peer. If there is none with the correct realm, it looks at the entries listed here.

Field
Description
Add Inbound Device Authentication

You can add a device’s authentication credentials to the list of entries against which the Call Server checks device credentials.

To add a device authentication:

1. Go to Service Config > Access Control > Device Authentication.
2. Click the Add icon.
3. In Add Device Authentication Credentials, complete the fields as described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Authentication</td>
<td>The name that the device includes in registration and signaling requests or responses to authentication challenges.</td>
</tr>
<tr>
<td>Name</td>
<td>The name that the device includes in registration and signaling requests or responses to authentication challenges.</td>
</tr>
<tr>
<td>Note: The name and password for a device are whatever values the person who configured the device specified. They don’t uniquely identify a specific device; multiple devices can have the same name and password.</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>The password that the device includes in registration and signaling requests or responses to authentication challenges.</td>
</tr>
<tr>
<td>Confirm password</td>
<td>The password that the device includes in registration and signaling requests or responses to authentication challenges.</td>
</tr>
</tbody>
</table>

Edit Device Authentication

You can edit a selected device’s authentication credentials as needed.

To edit device authentication:

1. Go to Service Config > Access Control > Device Authentication.
2  Select the device to edit.
3  Click the Edit icon.
4  In **Edit Device Authentication Credentials**, revise the fields as described in the following table as needed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Authentication</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>The name that the device includes in registration and signaling requests or responses to authentication challenges.</td>
</tr>
<tr>
<td><strong>Note:</strong> The name and password for a device are whatever values the person who configured it specified. They don’t uniquely identify a specific device; multiple devices can have the same name and password.</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>The password that the device includes in registration and signaling requests or responses to authentication challenges.</td>
</tr>
<tr>
<td>Confirm password</td>
<td></td>
</tr>
</tbody>
</table>
Site Topology

This section provides an introduction to working with the Polycom® RealPresence® DMA® system site topology. It includes:

- Site Topology
- Sites
- Network Clouds
- Site Links
- Site-to-Site Exclusions
- Territories
Site Topology

Within your Polycom environment, both the RealPresence Resource Manager system and RealPresence DMA systems require a site topology to be configured. If your environment includes integrated RealPresence Resource Manager and RealPresence DMA systems, you must use the RealPresence Resource Manager system to manage the site topology. When integrated with a RealPresence Resource Manager system, the RealPresence DMA system inherits all site topology settings. If a RealPresence DMA system is integrated with a RealPresence Resource Manager system, the site topology settings within the DMA system are read-only.

Site topology information logically describes your network and its interfaces to other networks, including the following elements:

- **Site**—A local area network (LAN) that generally corresponds with a geographic location such as an office or plant. A site contains one or more network subnets, so a device’s IP address identifies the site to which it belongs.
- **Network cloud**—A Multiprotocol Label Switching (MPLS) network cloud defined in the site topology. An MPLS network is a private network that links multiple locations and uses label switching to tag packets with origin, destination, and quality of service (QOS) information.
- **Site link**—A network connection between two sites or between a site and an MPLS network cloud.
- **Site-to-site exclusion**—A site-to-site connection that the site topology doesn’t permit a voice or video call to use.
- **Territory**—A collection of one or more sites for which a Polycom RealPresence DMA cluster is responsible. Territories serve multiple purposes in a Polycom RealPresence DMA system deployment.

The system installs with a default site topology with sites, subnets, and a site link that allow for endpoint registration and call routing (both multipoint and point-to-point).

Site topology information provides a logical model representation of a network topology, not necessarily a fully accurate literal representation of a full network.

**Shared Site Topology for Integrated Polycom Systems**

If you have integrated a RealPresence Resource Manager system with a RealPresence DMA system, you must use the RealPresence Resource Manager system to manage the site topology. When integrated with a RealPresence Resource Manager system, the RealPresence DMA system inherits all site topology settings.

**Bandwidth Management**

Once you model a site topology to represent your physical network, you can use it to manage bandwidth between your sites, preventing conference traffic from saturating the network.
Before the RealPresence DMA system routes a call, it considers the source and destination IP addresses in the site topology and determines a media path from the source subnet to the destination subnet, taking into account the existing calls and bandwidth restrictions along that path. If sites or site links have bandwidth restrictions, the system reduces the call rate of the call at the time of call setup so that it meets those restrictions, if possible. If the media path is already saturated with other conference traffic, the RealPresence DMA system rejects the call attempt.

Cascade for Bandwidth Conferences

For a conference with cascading for bandwidth enabled, the RealPresence DMA system uses the site topology information to route calls to the nearest eligible MCU (based on pools and pool orders) that has available capacity and to create the cascade links between MCUs.

Note: Cascading for bandwidth uses a hub-and-spoke configuration so that each cascaded MCU is only one link away from the “hub” MCU, which hosts the conference. The conference is hosted on the same MCU that would have been chosen in the absence of cascading, using the pool order applicable to the conference.
The cascade links between MCUs must use H.323 signaling. For conferences with cascading enabled, the Polycom RealPresence DMA system selects only MCUs that have H.323 signaling enabled.
This cascade link requirement doesn't affect endpoints, which may dial in using SIP (assuming the MCUs and the Polycom RealPresence DMA system are also configured for SIP signaling).

Supercluster Assignments

Within a RealPresence DMA system, cluster responsibility is determined via the site topology. If your RealPresence DMA system is superclustered, site topology data only needs to be created (or obtained from a RealPresence Resource Manager system) on one cluster of the superclusters. The data is replicated across the supercluster.

Configure Site Topology

You can configure your site topology in the RealPresence DMA system.

To configure your site topology in the RealPresence DMA system:

1. Go to Service Config > Site Topology > Network Clouds.
   Initially, the list of sites contains only an entry named Internet/VPN, which can’t be edited.

2. For each site in your network topology, do the following:
   a. In the Actions list, click Add.
   b. In the Add Site dialog, complete the General Info section. See Add a Site.
   c. To enable IP calls to/from the site, complete the ISDN Number Assignment, H.323 Routing and/or SIP Routing sections.
   d. In the Subnets section, specify the subnet or subnets that make up the site. See Add a Subnet.
   e. Click OK.
3 Go to Service Config > Site Topology > Territories.
   The list of territories contains an entry named Default RealPresence DMA Territory. It’s assigned to this RealPresence DMA system cluster. You can edit this entry, including changing its name and assigning sites to it.

4 Edit the Default RealPresence DMA Territory entry:
   a Select the entry and, in the Actions list, click Edit.
      The Edit Territory dialog appears.
   b In the Territory Info section, change the name and description for this territory if desired. Assign a primary and backup cluster for the territory, and elect whether to host conference rooms in this territory (the primary and backup cluster must be licensed for this capability).
   c In the Associated Sites section, add all the sites to the territory. See Edit a Territory.
   d Click OK.

5 Add other territories by clicking Add in the Actions list and completing the same settings in the Add Territory dialog.

6 Go to Service Config > Site Topology > Site Links, and for each direct link between sites, do the following:
   a In the Actions list, click Add.
   b In the Add Site Link dialog, define the link. See Add a Site Link.
   c Click OK.

7 Go to Service Config > Site Topology > Network Clouds, and for each MPLS network cloud in your network topology, do the following:
   a In the Actions list, click Add.
      The Add Network Cloud dialog appears.
   b In the Cloud Info section, enter a name and description for the cloud.
   c In the Linked Sites section, display the sites you defined. See Add a Network Cloud.
   d Select the first site linked to this cloud and click the arrow button to move it to the Linked Sites list.
      The Add Site Link dialog appears.
   e Define the link. See Add a Site Link.
   f Repeat the previous two steps for each additional site linked to this cloud.
   g Click OK.

8 Go to Service Config > Site Topology > Site-to-Site Exclusions, and for each exclusion in your network topology, do the following:
   a In the Actions list, click Add.
   b Complete the Add Site-to-Site Exclusions wizard. See Add a Site-to-Site Exclusion.

Your site topology information is complete. For a conference with cascading for bandwidth enabled, the RealPresence DMA system can use it to route calls to the nearest eligible MCU (based on pools and pool orders) that has available capacity and to create the cascade links between MCUs.

Note: If in the future you integrate this system with a RealPresence Resource Manager system, the site topology information from the RealPresence Resource Manager system will replace the information you entered.
Embedded DNS

In a superclustered configuration, the clusters that make up the supercluster automatically take over for each other in the event of an outage. In order to gain the full benefit of this feature, however, the endpoints that are registered to each cluster must re-register to a new cluster when the new cluster takes over.

This can be accomplished by specifying the gatekeeper or SIP proxy that each endpoint will register to as a site’s domain name, rather than an IP address. Then, when there is a failover, the DNS A record for that site’s domain name can be mapped to a different IP address, changing the Call Server that each endpoint is registered to.

The embedded DNS capability of the Polycom RealPresence DMA system automates this procedure. Each Polycom RealPresence DMA server hosts its own embedded DNS server. It publishes a DNS CNAME record for each site. That CNAME record maps to the active cluster with which endpoints at the site should register. Whenever responsibility for the site moves from one cluster to another, the change is automatically published by the embedded DNS server. Endpoints will automatically re-register to the correct cluster.

**Note:** The embedded DNS functionality is not supported in an IPv6 environment.

You can enable these embedded DNS servers on the Embedded DNS page. This is a supercluster-wide setting.

Embedded DNS is enabled by default for newly installed RealPresence DMA systems. In its default configuration, the Call server sub-domain controlled by DMA system field is populated with the default sub-domain video.local. The system acts as an initial DNS server, resolving the FQDN dma.video.local to the virtual IPv4 address of the local cluster. If you change the sub-domain to a custom value, the embedded DNS service resolves dma.<newsubdomain> to the IP address of the cluster.

If you wish to use this feature, your enterprise DNS must place the Polycom RealPresence DMA supercluster in charge of resolving the sub-domain specified on this page. To do this, you must:

- Add NS records to your enterprise DNS so that it refers requests to resolve the site-based logical host name (see View the Site Information) to these embedded DNS servers.
- Configure your enterprise DNS to forward requests for names in the site-based logical host name to any of the clusters in the supercluster.

For more information, see [DNS Records for the Polycom RealPresence DMA System](#).
The following table describes the fields on the **Embedded DNS** page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable embedded DNS service</td>
<td>Enables the embedded DNS servers.</td>
</tr>
<tr>
<td>Call server sub-domain controlled by RealPresence DMA</td>
<td>The fully qualified domain name of the enterprise domain for which the RealPresence DMA system is to provide DNS. For instance, for the base domain example.com, the sub-domain that the RealPresence DMA system services might be: callservers.example.com This is the logical Call Server domain name for which you must create NS records in your enterprise DNS. And this is the domain name that the system combines with each site name to form the logical FQDN that endpoints in each site should register to.</td>
</tr>
</tbody>
</table>

**Enable DNS Publishing**

You can enable Embedded DNS publishing on the **Embedded DNS** page.

To enable DNS publishing:

1. Be sure you’ve added the required NS records, one for each cluster in the supercluster, to your enterprise DNS and have configured it to forward requests for names in the logical Call Server domain to any of the clusters in the supercluster.

2. Go to **Service Config > Embedded DNS**.

3. Click **Enable embedded DNS service**.

4. In the **Call server sub-domain controlled by RealPresence DMA** field, enter the logical Call Server domain name (the enterprise domain for which the RealPresence DMA system is to provide DNS) and click **Update**.

5. Reconfigure your endpoints to register to the correct domain name for their site.

To determine the correct domain name for a site, go to **Service Config > Site Topology > Sites**, select the site, and click **Site Information**. The **Logical host name** field displays the correct domain name. It takes the form:

`callservers.example.com`<site name>.

For instance, if the fully qualified domain name for the logical Call Server domain is callservers.example.com, the correct domain name for endpoints in the paris site is:

`callserver-paris.callservers.example.com`

**Note:** If you have a Polycom RealPresence Resource Manager system integrated with the RealPresence DMA system, make sure that in its **Edit DMA** dialog, **Support DMA Supercluster** is selected. Enter all network/DNS-related information in all lower case to avoid possible case-sensitivity issues with various devices and ensure interoperability.
Working with Site Topology

If you have integrated a Polycom RealPresence Resource Manager system with a RealPresence DMA system, the system inherits all site topology settings from the RealPresence Resource Manager system and you must use the RealPresence Resource Manager system to manage the site topology. You cannot edit site topology information from the RealPresence DMA system. If the RealPresence DMA system is not integrated, you can enter site information from its web user interface.

Sites

The Internet/VPN and Default Site entries are provided with a new installation of the RealPresence DMA system.

The Internet/VPN entry always exists and cannot be edited or deleted. It cannot be assigned to a territory or controlled by a cluster. Endpoints whose subnet is not in any defined site in the enterprise network are considered to be in the Internet/VPN site. They can register to a cluster only if site-less registrations are allowed (see Registration Policy).

The Default Site entry has no restrictions. This site is configured to route SIP calls through a SIP-aware firewall, and includes three subnets that together cover the private IPv4 address space.

The protocol-specific routing settings for a site determine whether and how calls from that site can traverse the firewall to reach endpoints outside the enterprise network:

- Through a transparent firewall
- Through the specified Session Border Controller (SBC)
- Not at all

The site’s routing settings are used when the dial string is resolved by a dial rule using the Resolve to external address or Resolve to IP address action. See Dial Plans.

Alternatively, you can add an H.323 SBC (see External H.323 Session Border Controllers) or a SIP peer (see External SIP Peers) that can only be reached by dialing a specific prefix or prefixes. A dial string beginning with such a prefix can be resolved by the dial rule using the Resolve to service prefix action.

View the Site List

You can view a list of sites within your system’s site topology.

To view the site list:

» Go to Service Config > Site Topology > Sites.

The following table describes the fields in the list.
View the Site Information

You can view information about the selected site, including which subnets are associated with it and counts of the devices it contains.

To view the site information:

1. Go to Service Config > Site Topology > Sites.
2. Select the site of which you want to view detailed information.
3. In the ACTIONS list, select Site Information.

The following table describes the fields in the dialog, all of which are read-only.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Site Info | Name of the site.  
**Note:** If the system's embedded DNS service is enabled (see Embedded DNS), the system uses the site name to create the Logical host name (see below). Naming recommendations:  
- Use site names that contain only characters permitted in a host name (letters, numbers, and internal hyphens).  
- Enter network/DNS-related information in all lower case to avoid possible case-sensitivity issues with various devices and ensure interoperability. |

- Description | A brief description of the site. |
Add a Site

You can define a new site in the Polycom RealPresence DMA system's site topology and specify which subnets are associated with it.

**Note:** Enter all network/DNS-related information in all lower case to avoid possible case-sensitivity issues with various devices and ensure interoperability.

To add a new site:

1. Go to **Service Config > Site Topology > Sites**.
2. In the **Actions** list, click **Add**.

### Field | Description
--- | ---
Logical host name | If the system's embedded DNS service is enabled (see Embedded DNS), this is the logical FQDN that endpoints in this site should register to. The system generates this by combining "callserver," the site name, and the value specified in the **Call server sub-domain controlled by RealPresence DMA** field on the Embedded DNS page. If the site name contains a character not permitted in a host name, the system replaces it with a dash (hyphen) followed by the hex code of the ASCII character. For instance, if the site is named "paris (north)" and the call server sub-domain is "callservers.example.com," the logical host name would be: callserver-paris-20-28north-29.callservers.example.com

### Device Types

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCUs</td>
<td>The number of MCUs in the site.</td>
</tr>
<tr>
<td>DMAs</td>
<td>The number of Polycom RealPresence DMA systems in the site.</td>
</tr>
<tr>
<td>VBPs</td>
<td>The number of Polycom Video Border Proxy NAT/firewall traversal appliances in the site.</td>
</tr>
<tr>
<td>Endpoints</td>
<td>The number of registered endpoints in the site.</td>
</tr>
<tr>
<td>Subnets</td>
<td>A list of the subnets in the site.</td>
</tr>
</tbody>
</table>
3. Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Info</strong></td>
<td></td>
</tr>
<tr>
<td><strong>General Settings</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Site name                  | A meaningful name for the site (up to 128 characters). **Note:** If the system’s embedded DNS service is enabled (see Embedded DNS), the system uses the site name to create the Logical host name (see View the Site Information). Polycom recommends:  
  • Using site names that contain only characters permitted in a host name (letters, numbers, and internal hyphens).  
  • Entering network/DNS-related information in all lower case to avoid possible case-sensitivity issues with various devices and ensure interoperability. |
| Description                | A brief description of the site (up to 200 characters).                                                                                       |
| **Bandwidth Settings**     |                                                                                                                                               |
| Max total bandwidth (Mbps) | The total bandwidth limit for voice and video calls. If not selected, voice and video calls can use all of the available bandwidth.  
  This setting lets you restrict voice and video calls to only a portion of the available bandwidth, ensuring that some bandwidth always remains available for other network traffic. |
| Max per-call bit rate (kbps) | The per-call bit rate limit for voice and video calls.  
  When you specify both the bandwidth and bit rate limits, the dialog shows you how many calls at that bit rate the specified bandwidth limit supports. The value of the Bit rate to bandwidth conversion factor setting on the Call Server Settings page is used in this calculation. |
| **Territory Settings**     |                                                                                                                                               |
| Territory                  | Assigns the site to a territory, and thus to a Polycom RealPresence DMA cluster.                                                              |
Working with Site Topology

**ISDN Number Assignment**

**Assignment method**

The ISDN number assignment method for the devices in this site. The numbers being assigned are endpoint aliases in the form of E.164 numbers, which can be dialed by both IP endpoints registered to the Call Server and ISDN endpoints dialing in through an ISDN gateway.

The assignment options are:

- **No assignment.** Select this option when you don’t want to define a range of E.164 aliases for the site.
- **Manual assignment.** Select this option to define a range (or ranges) of E.164 aliases for the site, but not automatically assign those aliases to endpoints.
- **Automatic assignment.** Select this option to define a range (or ranges) of E.164 aliases for the site and automatically assign those aliases to endpoints that register without an alias.

After an E.164 alias is assigned to an endpoint, it’s reserved for use as long as that endpoint remains registered with the Polycom RealPresence DMA system.

If you do not enable **Automatic assignment**, you can manually add E.164 aliases to endpoints (see ). And endpoints will have any aliases with which they register.

**Dialing method**

The ISDN inward dialing method for the site:

- **DID (Direct Inward Dial).** Select this option if your ISDN gateway is provisioned with a range of phone numbers from the ISDN service provider, and each of these numbers will be assigned to an endpoint as an alias.
- **Gateway Extension Dialing.** Select this option if your ISDN gateway’s ISDN connection is provisioned with a single gateway phone number from the ISDN service provider, and endpoints will be assigned an extension (E.164 alias) that’s internal to the company and doesn’t correspond to any number that can be dialed on the PSTN.

Endpoints can be dialed from the PSTN by dialing the ISDN gateway phone number, followed by a delimiter (usually a #) and the extension number. The gateway receives the full number from the PSTN and dials only the extension number on the IP network.

**ISDN Outbound Dialing**

**Override ITU dialing rules**

Check this box to override the standard dialing rules, established by the International Telecommunications Union, when dialing out using an ISDN gateway.

The default setting, which does not override ITU dialing rules, is usually accurate for placing outbound calls. Enable this setting if you find that ISDN gateway calls from registered endpoints in this site are unsuccessful.

**PBX access code**

The code needed to access the ISDN/PSTN network through the site’s PBX when dialing out.

**Country code**

The country code for the site’s location. Click the CC button to select from a list of countries.

To apply ITU dialing rules, the system must compare the country code of the gateway site with the country code of the call’s destination.
### Working with Site Topology

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Area code</strong></td>
<td>The city or area code for the site’s location. Leading zeroes are optional. For example, the city code for Paris is 01, but you can enter either 01 or 1 in this field. To apply ITU dialing rules, the system must compare the area code of the gateway site with the area code of the call’s destination.</td>
</tr>
<tr>
<td><strong>Always dial area code</strong></td>
<td>Specifies that the area code should always be included in the phone number.</td>
</tr>
<tr>
<td><strong>Always dial national prefix</strong></td>
<td>Specifies that the national prefix should always be included in the phone number.</td>
</tr>
<tr>
<td><strong>Length of subscriber number</strong></td>
<td>The number of digits in a phone number. For example, in the United States and other areas using the North American Numbering Plan (NANP), subscriber numbers have seven digits.</td>
</tr>
</tbody>
</table>

**ISDN Range Assignment (for DID dialing method)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Length of call line identifier</strong></td>
<td>The number of digits in the Call Line Identifier (CLID), which is the dialed number. The maximum is 17. For example, in the United States, the number of digits in the CLID is often 7 for outside local calls and 11 for callers in a different area code.</td>
</tr>
<tr>
<td><strong>Length of short phone number</strong></td>
<td>The number of digits in the short form of the dialing number. For example, in the United States, internal extensions are usually four or five digits.</td>
</tr>
</tbody>
</table>

**ISDN Number Ranges**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ISDN gateway number</strong></td>
<td>An ISDN gateway phone number for the site. This field is just for your reference. It’s not used by the software to process calls. If the site has more than one ISDN gateway, you’ll need to know their access numbers and determine how to instruct inbound users to call.</td>
</tr>
<tr>
<td><strong>E.164 start</strong></td>
<td>The beginning of the range of E.164 extensions associated with the site.</td>
</tr>
<tr>
<td><strong>E.164 end</strong></td>
<td>The end of the range of E.164 extensions associated with the site. The start and end numbers in the range should be entered with the same number of digits.</td>
</tr>
</tbody>
</table>

**H.323 Routing**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Internet calls are not allowed</strong></td>
<td>Disables H.323 calls to the internet.</td>
</tr>
<tr>
<td><strong>Allowed via H.323-aware firewall</strong></td>
<td>Allows H.323 calls to the internet through a firewall.</td>
</tr>
<tr>
<td><strong>Allowed via H.323-aware SBC or ALG</strong></td>
<td>Enables H.323 calls to the internet through the specified session border controller (SBC) or application layer gateway (ALG).</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Call signaling address (IPv4)</td>
<td>The call signaling address for the H.323 SBC or ALG.</td>
</tr>
<tr>
<td>Port</td>
<td>The call signaling port for the H.323 SBC or ALG.</td>
</tr>
<tr>
<td><strong>SIP Routing</strong></td>
<td></td>
</tr>
<tr>
<td>Internet calls are not allowed</td>
<td>Enables SIP calls to the internet.</td>
</tr>
<tr>
<td>Allowed via SIP-aware firewall</td>
<td>Enables calls to the internet through a firewall.</td>
</tr>
<tr>
<td>Allowed via SIP-aware SBC or ALG</td>
<td>Enables SIP calls to the internet through the specified session border controller (SBC) or application layer gateway (ALG).</td>
</tr>
<tr>
<td>Call signaling address (IPv4)</td>
<td>The call signaling address for the SBC or ALG.</td>
</tr>
<tr>
<td>Port</td>
<td>The call signaling port for the SBC or ALG.</td>
</tr>
<tr>
<td><strong>Subnets</strong></td>
<td>Lists the subnets in the site. Click Add to add a subnet. Select a subnet in the table and click Edit or Delete to modify or remove it.</td>
</tr>
<tr>
<td>Subnet Name</td>
<td>The unique name of the subnet.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the subnet. You can define overlapping subnets; larger subnets can contain smaller ones. When the system determines which subnet a given IP address belongs to, it chooses the subnet with the longest IP address match. For example: subnet1 = 10.0.0.0/8 subnet2 = 10.33.24.0/24 The IP address 10.33.24.70 belongs to subnet2. The IP address 10.22.23.70 belongs to subnet1.</td>
</tr>
<tr>
<td>Subnet Mask Length</td>
<td>The CIDR (Classless Inter-Domain Routing) prefix size value (the number of leading 1 bits in the routing prefix mask). This value, together with the IP Address, defines the subnet. For IPv4, a value of 24 is equivalent to specifying a dotted-quad subnet mask of 255.255.255.0. A value of 16 is equivalent to specifying a subnet mask of 255.255.0.0. You can use subnet mask lengths of up to 32 bits; a 32-bit subnet mask allows you to specify a single device.</td>
</tr>
<tr>
<td>Max Total Bandwidth (Mbps)</td>
<td>The total bandwidth limit for voice and video calls.</td>
</tr>
<tr>
<td>Max Per-Call Bit Rate (kbps)</td>
<td>The per-call bit rate limit for voice and video calls. When you specify both the bandwidth and bit rate limits, the dialog shows you how many calls at that bit rate the specified bandwidth limit supports. The value of the Bit rate to bandwidth conversion factor setting on the Call Server Settings page is used in this calculation.</td>
</tr>
</tbody>
</table>

4. Complete the required fields and click OK.
**Edit a Site**

You can edit a site in the Polycom RealPresence DMA system’s site topology and add or edit a subnet associated with the site.

**Note:** Enter all network/DNS-related information in all lower case to avoid possible case-sensitivity issues with various devices and ensure interoperability.

### To edit a site:

1. Go to Service Config > Site Topology > Sites.
2. Choose a site from the list, and click **Edit** in the **Actions** list.

   The **Edit Site** dialog displays the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Info</strong></td>
<td></td>
</tr>
<tr>
<td>Site name</td>
<td>A meaningful name for the site (up to 128 characters). <strong>Note:</strong> If the system’s embedded DNS service is enabled (see Embedded DNS), the system uses the site name to create the <strong>Logical host name</strong> (see View the Site Information). Polycom recommends: • Using site names that contain only characters permitted in a host name (letters, numbers, and internal hyphens). • Entering network/DNS-related information in all lower case to avoid possible case-sensitivity issues with various devices and ensure interoperability.</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the site (up to 200 characters).</td>
</tr>
<tr>
<td><strong>Bandwidth Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Max total bandwidth (Mbps)</td>
<td>The total bandwidth limit for voice and video calls. If not selected, voice and video calls can use all of the available bandwidth. This setting lets you restrict voice and video calls to only a portion of the available bandwidth, ensuring that some bandwidth always remains available for other network traffic.</td>
</tr>
<tr>
<td>Max per-call bit rate (kbps)</td>
<td>The per-call bit rate limit for voice and video calls. When you specify both the bandwidth and bit rate limits, the dialog shows you how many calls at that bit rate the specified bandwidth limit supports. The value of the <strong>Bit rate to bandwidth conversion factor</strong> setting on the Call Server Settings page is used in this calculation.</td>
</tr>
<tr>
<td><strong>Territory Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Territory</td>
<td>Assigns the site to a territory, and thus to a Polycom RealPresence DMA cluster.</td>
</tr>
</tbody>
</table>
## Working with Site Topology

### ISDN Number Assignment

<table>
<thead>
<tr>
<th>Assignment method</th>
<th>The ISDN number assignment method for the devices in this site. The numbers being assigned are endpoint aliases in the form of E.164 numbers, which can be dialed by both IP endpoints registered to the Call Server and ISDN endpoints dialing in through an ISDN gateway.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>No assignment</strong></td>
<td>Select this option when you don’t want to define a range of E.164 aliases for the site.</td>
</tr>
<tr>
<td><strong>Manual assignment</strong></td>
<td>Select this option to define a range (or ranges) of E.164 aliases for the site, but not automatically assign those aliases to endpoints.</td>
</tr>
<tr>
<td><strong>Automatic assignment</strong></td>
<td>Select this option to define a range (or ranges) of E.164 aliases for the site and automatically assign those aliases to endpoints that register without an alias.</td>
</tr>
</tbody>
</table>

After an E.164 alias is assigned to an endpoint, it’s reserved for use as long as that endpoint remains registered with the Polycom RealPresence DMA system.

If you decide not to enable **Automatic assignment**, you can always manually add E.164 aliases to endpoints from the **Endpoints** page (see **Edit an Endpoint**). And endpoints will have any aliases with which they register.

### ISDN Outbound Dialing

<table>
<thead>
<tr>
<th>Override ITU dialing rules</th>
<th>Select this check box to override the standard dialing rules, established by the International Telecommunications Union, when dialing out using an ISDN gateway. The default setting, which does not override ITU dialing rules, is usually accurate for placing outbound calls. Enable this setting if you find that ISDN gateway calls from registered endpoints in this site are unsuccessful.</th>
</tr>
</thead>
<tbody>
<tr>
<td>PBX access code</td>
<td>The code needed to access the ISDN/PSTN network through the site’s PBX when dialing out.</td>
</tr>
<tr>
<td>Country code</td>
<td>The country code for the site’s location. Click the CC button to select from a list of countries. To apply ITU dialing rules, the system must compare the country code of the gateway site with the country code of the call’s destination.</td>
</tr>
</tbody>
</table>
### Working with Site Topology

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Area code                         | The city or area code for the site's location. Leading zeroes are optional. For example, the city code for Paris is 01, but you can enter either 01 or 1 in this field.  
To apply ITU dialing rules, the system must compare the area code of the gateway site with the area code of the call's destination. |
| Always dial area code             | Specifies that the area code should always be included in the phone number.                                                                                                                                   |
| Always dial national prefix       | Specifies that the national prefix should always be included in the phone number.                                                                                                                             |
| Length of subscriber number       | The number of digits in a phone number. For example, in the United States and other areas using the North American Numbering Plan (NANP), subscriber numbers have seven digits.                                    |

#### ISDN Range Assignment (for DID dialing method)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Length of call line identifier    | The number of digits in the Call Line Identifier (CLID), which is the dialed number. The maximum is 17.  
For example, in the United States, the number of digits in the CLID is often 7 for outside local calls and 11 for callers in a different area code. |
| Length of short phone number      | The number of digits in the short form of the dialing number.  
For example, in the United States, internal extensions are usually four or five digits.                                                                                                                |
| ISDN Number Ranges                | The number ranges available for assignment to endpoints in the site.  
Click Add to add a new range of numbers. Click Edit or Delete to change or delete the selected range.  
The start and end numbers in the range should be entered with the same number of digits. If the range is 303-223-1000 to 1999, enter 3032231000 and 3032231999. |

#### ISDN Range Assignment (for gateway extension dialing method)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| ISDN gateway number               | An ISDN gateway phone number for the site. This field is just for your reference. It’s not used by the software to process calls.  
If the site has more than one ISDN gateway, you’ll need to know their access numbers and determine how to instruct inbound users to call. |
| E.164 start                       | The beginning of the range of E.164 extensions associated with the site.                                                                                                                                     |
| E.164 end                         | The end of the range of E.164 extensions associated with the site.  
The start and end numbers in the range should be entered with the same number of digits.                                                                                                               |

### H.323 Routing

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet calls are not allowed</td>
<td>Disables H.323 calls to the internet.</td>
</tr>
<tr>
<td>Allowed via H.323-aware firewall</td>
<td>Allows H.323 calls to the internet through a firewall.</td>
</tr>
<tr>
<td>Allowed via H.323-aware SBC or ALG</td>
<td>Enables H.323 calls to the internet through the specified session border controller (SBC) or application layer gateway (ALG).</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Call signaling address (IPv4)</td>
<td>The call signaling address for the H.323 SBC or ALG.</td>
</tr>
<tr>
<td>Port</td>
<td>The call signaling port for the H.323 SBC or ALG.</td>
</tr>
<tr>
<td><strong>SIP Routing</strong></td>
<td></td>
</tr>
<tr>
<td>Internet calls are not allowed</td>
<td>Disables SIP calls to the internet.</td>
</tr>
<tr>
<td>Allowed via SIP-aware firewall</td>
<td>Enables calls to the internet through a firewall.</td>
</tr>
<tr>
<td>Allowed via SIP-aware SBC or ALG</td>
<td>Enables SIP calls to the internet through the specified session border controller (SBC) or application layer gateway (ALG).</td>
</tr>
<tr>
<td>Call signaling address (IPv4)</td>
<td>The call signaling address for the SBC or ALG.</td>
</tr>
<tr>
<td>Port</td>
<td>The call signaling port for the SBC or ALG.</td>
</tr>
<tr>
<td><strong>Subnets</strong></td>
<td></td>
</tr>
<tr>
<td>Subnet Name</td>
<td>The unique name of the subnet.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the subnet. You can define overlapping subnets; larger subnets can contain smaller ones. When the system determines which subnet a given IP address belongs to, it chooses the subnet with the longest IP address match. For example: subnet1 = 10.0.0.0/8 subnet2 = 10.33.24.0/24 The IP address 10.33.24.70 belongs to subnet2. The IP address 10.22.23.70 belongs to subnet1.</td>
</tr>
<tr>
<td>Subnet Mask Length</td>
<td>The CIDR (Classless Inter-Domain Routing) prefix size value (the number of leading 1 bits in the routing prefix mask). This value, together with the IP Address, defines the subnet. For IPv4, a value of 24 is equivalent to specifying a dotted-quad subnet mask of 255.255.255.0. A value of 16 is equivalent to specifying a subnet mask of 255.255.0.0. You can use subnet mask lengths of up to 32 bits; a 32-bit subnet mask allows you to specify a single device.</td>
</tr>
<tr>
<td>Max Total Bandwidth (Mbps)</td>
<td>The total bandwidth limit for voice and video calls.</td>
</tr>
<tr>
<td>Max Per-Call Bit Rate (kbps)</td>
<td>The per-call bit rate limit for voice and video calls. When you specify both the bandwidth and bit rate limits, the dialog shows you how many calls at that bit rate the specified bandwidth limit supports. The value of the bit rate to bandwidth conversion factor setting on the Call Server Settings page is used in this calculation.</td>
</tr>
</tbody>
</table>

3. Complete the required fields and click OK.
Add a Subnet

You can add subnets to the site you’re adding or editing. You cannot assign the same subnet to more than one site.

To add a subnet:

1. Go to Service Config > Site Topology > Sites.
2. In the Actions list, click Add to add a new site, or Edit to edit an existing site.
3. In the Add Site or Edit Site dialog, select the Subnets section.
4. Click Add.
5. In the Add Subnet dialog, edit the fields in the following table as required.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the subnet. Required and must be unique.</td>
</tr>
<tr>
<td>IP address</td>
<td>The IP address of the subnet.</td>
</tr>
<tr>
<td>Subnet mask length</td>
<td>The CIDR (Classless Inter-Domain Routing) prefix size value (the number of</td>
</tr>
<tr>
<td></td>
<td>leading 1 bits in the routing prefix mask). This value, together with the</td>
</tr>
<tr>
<td></td>
<td>IP Address, defines the subnet.</td>
</tr>
<tr>
<td></td>
<td>For IPv4, a value of 24 is equivalent to specifying a dotted-quad subnet</td>
</tr>
<tr>
<td></td>
<td>mask of 255.255.255.0. A value of 16 is equivalent to specifying a dotted-quad</td>
</tr>
<tr>
<td></td>
<td>subnet mask of 255.255.0.0.</td>
</tr>
<tr>
<td>Max total bandwidth (Mbps)</td>
<td>The total bandwidth limit for voice and video calls. If not specified, the</td>
</tr>
<tr>
<td></td>
<td>site limit applies.</td>
</tr>
<tr>
<td>Max per-call bit rate (kbps)</td>
<td>The per-call bit rate limit for voice and video calls. If not specified,</td>
</tr>
<tr>
<td></td>
<td>the site limit applies.</td>
</tr>
<tr>
<td></td>
<td>When you specify both the bandwidth and bit rate limits, the dialog shows</td>
</tr>
<tr>
<td></td>
<td>you how many calls at that bit rate the specified bandwidth supports. The</td>
</tr>
<tr>
<td></td>
<td>value of the Bit rate to bandwidth conversion factor setting on the Call</td>
</tr>
<tr>
<td></td>
<td>Server Settings page is used in this calculation.</td>
</tr>
</tbody>
</table>

6. Click OK.

Edit a Subnet

You can edit a subnet associated with a site. You cannot assign the same subnet to more than one site.

To edit a subnet:

1. Go to Service Config > Site Topology > Sites.
2. Choose a site from the list, and click Edit in the Actions list.
3. In the Edit Site dialog, select the Subnets section.
4. Click Edit.
5. In the Edit Subnet dialog, edit the fields in the following table as required.
Network Clouds

You can define MPLS (Multiprotocol Label Switching) network clouds in your site topology. MPLS is a special technology typically offered via a private WAN environment, providing more reliability than the Internet. If you are unsure if your enterprise has an MPLS network cloud, speak to your IT administrator.

If the RealPresence DMA system is integrated with a RealPresence Resource Manager system, it receives MPLS network information from that system, and this page is read-only. If not, you can enter MPLS network cloud information.

View Network Clouds

You can view a list of any network clouds you have added.

To view the network cloud list:

» Go to Service Config > Site Topology > Network Clouds.

The network cloud lists each cloud by name and description.

Add a Network Cloud

You can define a new MPLS network cloud in your system’s site topology.
To add a new network cloud:

1. Go to Service Config > Site Topology > Network Clouds.
2. In the Actions list, click Add.
3. In the Add Network Cloud dialog, edit the fields in the following table as required.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Info</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>A meaningful name for the cloud (up to 128 characters).</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the cloud (up to 200 characters).</td>
</tr>
<tr>
<td>Associated Sites</td>
<td></td>
</tr>
<tr>
<td>Search Sites</td>
<td>Enter search string or leave blank to find all sites.</td>
</tr>
<tr>
<td>Search Result</td>
<td>Lists sites found and shows the territory, if any, to which each belongs.</td>
</tr>
<tr>
<td></td>
<td>Select a site and click the right arrow to open the Add Site Link dialog (see Add a Site Link).</td>
</tr>
<tr>
<td>Associated Sites</td>
<td>Lists sites linked to the cloud and shows the territory, if any, to which each belongs.</td>
</tr>
</tbody>
</table>

4. Click OK.

**Edit a Network Cloud**

You can edit an MPLS network cloud in the Polycom RealPresence DMA system’s site topology.

To edit a network cloud:

1. Go to Service Config > Site Topology > Network Clouds.
2. Choose a network cloud from the list, and click Edit in the Actions list.
3. In the Edit Network Cloud dialog, edit the fields in the following table as required.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Info</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>A meaningful name for the cloud (up to 128 characters).</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the cloud (up to 200 characters).</td>
</tr>
<tr>
<td>Associated Sites</td>
<td></td>
</tr>
<tr>
<td>Search Sites</td>
<td>Enter search string or leave blank to find all sites.</td>
</tr>
</tbody>
</table>
Site Links

Links between sites must be configured in order to enable calls between sites. For an endpoint in site A to call an endpoint in site B, there must be a link path connecting site A and site B. A site link can connect two sites, or it can connect a site to an MPLS network cloud.

An initial site link is provided by default, named Default Site to Internet/VPN. It links the default site with the Internet/VPN site to allow call routing for a newly deployed system.

If the system is integrated with a RealPresence Resource Manager system, it receives this information from that system, and you cannot modify any site link information. If the RealPresence DMA system is not integrated with a RealPresence Resource Manager system, you can enter link information.

Add a Site Link

You can define a new site link in the Polycom RealPresence DMA system’s site topology. A link can connect two sites, or it can connect a site to an MPLS network cloud.

To add a new site link:

1. Go to Service Config > Site Topology > Site Links.
2. In the Actions list, click Add.
3. In the Add Site Link dialog, edit the fields in the following table as required.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A meaningful name for the link (up to 128 characters).</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the link (up to 200 characters).</td>
</tr>
<tr>
<td>From site</td>
<td>The originating site of the link.</td>
</tr>
<tr>
<td>To site</td>
<td>The destination site of the link.</td>
</tr>
</tbody>
</table>
Edit a Site Link

You can edit a site link in the Polycom RealPresence DMA system’s site topology. A link can connect two sites, or it can connect a site to an MPLS network cloud.

You can’t change the sites that a site link connects. To modify how sites are linked, delete the links to be removed and add the new links.

To edit a site link:

1. Go to Service Config > Site Topology > Site Links.
2. Choose a site from the list, and click Edit in the Actions list.
3. In the Edit Site Link dialog, edit the fields in the following table as required.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max total bandwidth (Mbps)</td>
<td>The total bandwidth limit for voice and video calls, which you set at the gateway or router.</td>
</tr>
<tr>
<td>Max per-call bit rate (kbps)</td>
<td>The per-call bit rate limit for voice and video calls, which you set at the gateway or router. When you specify both the bandwidth and bit rate limits, the dialog shows you how many calls at that bit rate the specified bandwidth supports. The value of the Bit rate to bandwidth conversion factor setting on the Call Server Settings page is used in this calculation.</td>
</tr>
</tbody>
</table>

4. Click OK.
Site-to-Site Exclusions

The Site-to-Site Exclusions are site-to-site connections that the site topology does not permit a call or session to use.

If the system is integrated with a RealPresence Resource Manager system, it receives this information from that system, and this page is read-only. If not, you can define exclusions.

View Site-to-Site Exclusions

You can view a list of any site-to-site exclusions that exist in your site topology.

To view the list:

» Go to Service Config > Site Topology > Site-to-Site Exclusions.

The following table describes the fields in the list.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Site</td>
<td>Name of one of the two sites connected by the excluded link.</td>
</tr>
<tr>
<td>To Site</td>
<td>Name of the other site.</td>
</tr>
</tbody>
</table>

Add a Site-to-Site Exclusion

You can define a new site-to-site exclusion in the Polycom RealPresence DMA system's site topology.

To add a site-to-site exclusion:

1. Go to Service Config > Site Topology > Site-to-Site Exclusions.
2. In the Actions list, click Add.
3. In Step 1 of the wizard, select the first site for the exclusion.
4. Click Next.
   If the site you want isn’t displayed in the list, you can search by site name or territory.
5. In Step 2 of the wizard, select the second site for the exclusion.
6. Click Next.
7. In Step 3 of the wizard, review the exclusion and click Done if it’s correct.

Territories

A territory contains one or more sites for which a Polycom RealPresence DMA cluster is responsible. By default, there is one territory named Default DMA Territory.

In a superclustered RealPresence DMA system deployment, additional territories allow you to assign different territories to different RealPresence DMA clusters and to specify a backup cluster for each territory to increase fault tolerance. If a territory’s primary cluster becomes unavailable for any reason, the backup cluster takes over the responsibilities for the territory.
Territories serve the following purposes:

- Sites are associated with territories, thus specifying which RealPresence DMA cluster is responsible for serving as the H.323 gatekeeper, SIP registrar, and SIP proxy for each site.
- Microsoft Active Directory integration is associated with a territory, thus specifying which RealPresence DMA cluster is responsible for connecting to the directory server, retrieving user and group data, and updating the shared supercluster data.
- Microsoft Exchange server integration (for calendaring service) is associated with a territory, thus specifying which RealPresence DMA cluster is responsible for integrating with the Exchange server and monitoring the Polycom Conferencing infrastructure mailbox.
- The RealPresence DMA system’s Conference Manager functionality is associated with territories, thus specifying which Polycom RealPresence DMA clusters are responsible for hosting conference rooms (VMRs). Up to three territories (and thus clusters) may have this responsibility.

If the system is integrated with a RealPresence Resource Manager system, it receives territory information from that system, and the Territories page is view-only. If not, you can modify the territory information.

**View the Territories List**

You can view the list of territories that have been added to your site topology.

To view the territories list:

1. Go to Service Config > Site Topology > Territories.
2. On the right, it displays information about the selected territory.

The following table describes the fields in the list.

<table>
<thead>
<tr>
<th>Column/Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the territory.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the territory.</td>
</tr>
<tr>
<td>Primary Cluster</td>
<td>The primary RealPresence DMA cluster responsible for this territory.</td>
</tr>
<tr>
<td>Backup Cluster</td>
<td>The backup RealPresence DMA cluster, if any, responsible for this territory.</td>
</tr>
<tr>
<td>Host Conference Rooms</td>
<td>Indicates whether this territory is used for hosting conference rooms (VMRs,</td>
</tr>
<tr>
<td></td>
<td>or virtual meeting rooms).</td>
</tr>
<tr>
<td><strong>Territory Summary</strong></td>
<td>Repeats the name and description of the selected territory.</td>
</tr>
<tr>
<td><strong>Associated Sites</strong></td>
<td>List the sites included in the selected territory.</td>
</tr>
</tbody>
</table>
To add a new territory:

1. Navigate to **Service Config > Site Topology > Territories**.
2. In the **Actions** list, click **Add**.
3. In the **Add Territory** dialog, edit the fields in the following table as required.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Territory Info</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>A meaningful name for the territory (up to 128 characters).</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the territory (up to 200 characters).</td>
</tr>
<tr>
<td>Primary cluster</td>
<td>The primary RealPresence DMA cluster responsible for this territory.</td>
</tr>
<tr>
<td>Backup cluster</td>
<td>The backup RealPresence DMA cluster, if any, responsible for this territory. You must have a supercluster consisting of at least two RealPresence DMA clusters in order to specify a backup.</td>
</tr>
<tr>
<td>Host conference rooms in this territory</td>
<td>Enables this territory to be used for hosting conference rooms (VMRs, or virtual meeting rooms). The territory's primary and backup clusters must both be enabled for conference room hosting. No more than three territories may have this capability enabled.</td>
</tr>
</tbody>
</table>

| **Associated Sites**         |                                                                            |
| Search sites                 | Enter search string or leave blank to find all sites.                      |
| Available sites              | Lists sites found and shows the territory, if any, to which each currently belongs. Selecting a site and moving it to the **Associated sites** list changes its territory assignment to this territory. |
| Associated sites             | Lists sites linked to this territory. Changes you make to this list aren’t implemented until you click **OK**. |

4. Click **OK**.

**Edit a Territory**

You can revise a territory in your system’s site topology as needed.

To edot a territory:

1. Go to **Service Config > Site Topology > Territories**.
2. Select the territory to edit.
3. Under **Actions**, click **Edit**.
4 Edit the fields in the following table as needed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Territory Info</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>A meaningful name for the territory (up to 128 characters).</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the territory (up to 200 characters).</td>
</tr>
<tr>
<td>Primary cluster</td>
<td>The primary RealPresence DMA cluster responsible for this territory.</td>
</tr>
<tr>
<td>Backup cluster</td>
<td>The backup RealPresence DMA cluster, if any, responsible for this territory.</td>
</tr>
<tr>
<td>You must have a supercluster consisting of at least two RealPresence DMA clusters in order to specify a backup.</td>
<td></td>
</tr>
<tr>
<td>Host conference rooms in this territory</td>
<td>Enables this territory to be used for hosting conference rooms (VMRs, or virtual meeting rooms).</td>
</tr>
<tr>
<td>The territory's primary and backup clusters must both be enabled for conference room hosting. No more than three territories may have this capability enabled.</td>
<td></td>
</tr>
<tr>
<td><strong>Associated Sites</strong></td>
<td></td>
</tr>
<tr>
<td>Search sites</td>
<td>Enter search string or leave blank to find all sites.</td>
</tr>
<tr>
<td>Available sites</td>
<td>Lists sites found and shows the territory, if any, to which each currently belongs.</td>
</tr>
<tr>
<td>Selecting a site and moving it to the <strong>Associated sites</strong> list changes its territory assignment to this territory.</td>
<td></td>
</tr>
<tr>
<td>Associated sites</td>
<td>Lists sites linked to this territory. Changes you make to this list aren’t implemented until you click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>

5 Click **OK**.
Users and Groups

This section provides an introduction to managing local and enterprise users and groups in the Polycom® RealPresence® DMA® system. It includes:

- User Roles and Access Privileges
- Users
- Groups
- Login Policy Settings
User Roles and Access Privileges

The Polycom RealPresence DMA system has four user roles, or classes of users, each with its own set of permissions. Every user account has one or more user roles, but only three of the four roles must be explicitly assigned.

User Roles

The following table describes the user roles. See User Access Privileges to view the system functions that are available to each user role.

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
</table>
| Administrator   | Responsible for the overall administration of the system. Can access all the pages except those reserved for auditors (must be an enterprise user to see enterprise reports, enterprise users, and groups).  
If you have a Polycom RealPresence Resource Manager system, assign this role to its login account. If API access for other clients is enabled, assign this role to the login account of any other API client that should have administrative rights and responsibilities.  
This role must be explicitly assigned by an Administrator. |
| Auditor         | Responsible for configuring logging and history record retention, and for managing logs. Can access all history reports.  
This role must be explicitly assigned by an Administrator.                                                                                                                                                                                                                   |
| Provisioner     | Responsible for the management of Conferencing User accounts.  
Can create or modify only users with no role other than Conferencing User, but can view all local users. Must be an enterprise user to view all enterprise users. Can view history reports.  
If you have a Polycom RealPresence Resource Manager system or any other API client, assign this role to its users who should have provisioning rights and responsibilities.  
This role must be explicitly assigned by an Administrator.                                                                                                                                                                                                                   |
| Conferencing User | Has been provisioned with a conference room (virtual meeting room, or VMR) or rooms and can host conferences. Cannot access the system management interface.  
This role is automatically present on all user accounts. It is not listed under Available Roles or explicitly assigned.  
For purposes of API access, the system identifies a subcategory of Conferencing User, the Conference Room Owner, who can monitor and control his or her conferences.                                                                 |

If your system is integrated with a Microsoft Active Directory, all enterprise users are automatically Conferencing Users. You can use enterprise groups to manage assignment of the other user roles.
Note: You must be an enterprise user (with the appropriate user role assignments) to see and work with enterprise users. A local user can only see other local users, regardless of user roles.

## User Access Privileges

The Polycom RealPresence DMA system has three user roles that provide access to the management and operations interface and the RealPresence Platform Application Programming Interface (API). The functions you can perform and parts of the interface you can access depend on your user role or roles, as shown in the following table.

<table>
<thead>
<tr>
<th>Menu/Icon</th>
<th>Admin</th>
<th>Provisioner</th>
<th>Auditor</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Home. Returns to the Dashboard.</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td><strong>Monitoring</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Calls</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Endpoints</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>High Availability Status</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Login Sessions¹</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Site Statistics¹</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Site Link Statistics¹</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Network Usage</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td><strong>User</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Users ²</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Login Policy Settings &gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local User Account</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local Password</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Session</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Banner</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management Access Settings</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Integrations</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DMAs</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>MCUs¹</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>RealPresence Resource Manager</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>External SIP Peers¹</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Menu/Icon</td>
<td>Admin</td>
<td>Provisioner</td>
<td>Auditor</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>External H.323 Gatekeepers¹</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>External H.323 SBCs¹</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft Active Directory³</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>External Skype Systems</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft Exchange Server</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Service Config</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conference Manager Settings &gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conference Settings</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conference Templates</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MCU Pools¹</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MCU Pool Orders¹</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shared Number Dialing</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IVR Prompt Sets</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIP Conference Factories</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Presence Publishing for Skype</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Call Server Settings</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Dial Plan &gt;</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dial Plans</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prefix Service</td>
<td>•</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>Hunt Groups</td>
<td>•</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>Domain Restrictions</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Site Topology &gt;</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sites¹</td>
<td>•</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>Site Links¹</td>
<td>•</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>Site-to-Site Exclusions¹</td>
<td>•</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>Network Clouds¹</td>
<td>•</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>Territories¹</td>
<td>•</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>SIP Settings</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>H.323 Settings</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WebRTC Settings</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Menu/Icon</td>
<td>Admin</td>
<td>Provisioner</td>
<td>Auditor</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>Access Control</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device Authentication</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Registration Policy</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Embedded DNS</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reports</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Call History</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Conference History</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Registration History</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Alert History</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>MS Active Directory Reports &gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Orphaned Groups and Users</td>
<td>*</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>Admin</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server &gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Settings</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>High Availability Settings</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time Settings</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Licenses</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logging Settings</td>
<td>*</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>SNMP Settings</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alert Settings</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>History Retention Settings</td>
<td>*</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>Backup Settings</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Settings</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certificates</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change Linux Root Password</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Log Files[^]{4}</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
</tbody>
</table>
### User Roles and Access Privileges

<table>
<thead>
<tr>
<th>Menu/Icon</th>
<th>Admin</th>
<th>Provisioner</th>
<th>Auditor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Troubleshooting Utilities &gt;</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Packet Capture</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ping</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Traceroute</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Top</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>I/O Stats</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAR</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTP Status</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software Upgrade</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backup and Restore</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shutdown and Restart</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Help</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Help Contents</td>
<td>•</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>RealPresence Platform API Documentation</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>About RealPresence DMA</td>
<td>•</td>
<td></td>
<td>•</td>
</tr>
</tbody>
</table>

- **Alerts/messages**
  - • • •

- **Refresh interval**
  - • • •

- **User role, e.g., Admin. Click to Change Password or Sign Out of the system.**
  - • • •

- **Help. Opens the online help for the page you’re viewing.**
  - • • •

1. Provisioners have view-only access.
2. Must be an enterprise user to see enterprise users. Provisioners cannot add or remove roles or endpoints, and cannot edit user accounts with explicitly assigned roles (Administrator, Provisioner, or Auditor), but can manage their conference rooms.
3. Must be an enterprise user to view this report.
4. Administrators cannot delete log archives.
Users

The Polycom® RealPresence® DMA® system recognizes two types of users: local and enterprise. 

Local users are those that you add manually to the RealPresence DMA system. When you manually add users, you assign them conference rooms and the specific roles they need to have.

Enterprise users are automatically added as RealPresence DMA system users when you integrate your system with a Microsoft® Active Directory (AD). This integration allows users with specific roles (Administrator, Auditor, or Provisioner) to log into the RealPresence DMA system with their Active Directory user names and passwords. The integration process can also automatically create conference rooms for Active Directory enterprise users based on the Active Directory field (such as phone number) that you specify.

Active Directory enterprise users are automatically assigned a Conferencing User role and display in the Users list. An administrator can assign them additional roles as required.

Note: You must be an enterprise user (with the appropriate user role assignments) to see and work with enterprise users. A local user can only see other local users, regardless of user roles.

In the Polycom RealPresence DMA system, you can manage local and enterprise users and different types of conference rooms and associate endpoints with specific users.

- Managing Users
- Conference Rooms
- Associated Endpoints

Managing Users

A newly installed system has two local user accounts: admin and rppuser. The rppuser account is populated with the factory default configuration, has the same default password as admin, and is not assigned any user roles. Five VMRs are assigned to the rppuser account, all of which are configured with factory default settings. You can use these VMRs to make test calls on a newly deployed system.

The admin account is a user account with Administrator privileges. Polycom recommends that, as part of initial system setup, you create a local user account for yourself with the Administrator role, log in using that account, and delete the admin user account. You can then create other local user accounts or integrate with an Active Directory and assign additional roles to the appropriate enterprise users.

If you plan to integrate with a Polycom RealPresence Resource Manager system, you must create a local user account for the RealPresence Resource Manager system, which enables it to log into the RealPresence DMA system’s RealPresence Platform API. This account should have administrator and provisioner roles.
The RealPresence Resource Manager user owns the conference rooms (VMRs) it creates for preset dial-out conferences (called *Anytime* conferences in the RealPresence Resource Manager system).

**Add a Local User**

You can add a local user to the RealPresence DMA system and assign additional roles to the user.

**Note:** If Cisco Codian MCUs are included in the Polycom RealPresence DMA system’s pool of conferencing resources, do not assign a chairperson passcode without also assigning a conference passcode. If a conference with only one passcode (either chairperson or conference) lands on a Codian MCU, all callers to the conference must enter that passcode.

**To add a local user:**

1. Go to **User > Users**.
2. Under **Actions** list, click **Add**.
3. Complete the fields in the following table as required.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Info</strong></td>
<td></td>
</tr>
<tr>
<td>First name</td>
<td>The local user’s first name.</td>
</tr>
<tr>
<td>Last name</td>
<td>The local user’s last name.</td>
</tr>
<tr>
<td>User ID</td>
<td>The local user’s login name.</td>
</tr>
<tr>
<td>Password</td>
<td>The local user’s system login password (not conference or chairperson passcode). This is the password that enables users with explicitly assigned roles to log into the system’s management interface. The password must satisfy the local password rules specified for the system.</td>
</tr>
<tr>
<td>Confirm password</td>
<td></td>
</tr>
<tr>
<td>Email address</td>
<td>The local user’s email address.</td>
</tr>
<tr>
<td>User pass-through to CDR</td>
<td>Optional value to put in the <em>userDataA</em> field of call detail records (CDRs) associated with this user. For example, this might be a user ID from some external system or database.</td>
</tr>
<tr>
<td>Account disabled</td>
<td>If selected, the user cannot host conferences (the user’s conference room or rooms are not available) and cannot access the system’s management interface. You can select the check box and still create the user account, but not activate it immediately.</td>
</tr>
</tbody>
</table>
Conference room territory
The territory to which the user’s conference rooms (virtual meeting rooms, or VMRs) are assigned.
A conference room's territory assignment determines which RealPresence DMA cluster hosts the room's conferences (the primary cluster for the territory, or its backup cluster if necessary).
If not selected, the user’s conference rooms are assigned as follows (in priority order listed):
• To the territory associated with the room specifically.
• To the territory associated with the Active Directory group the user belongs to (if more than one, the group that is alphabetically first).
• To the system’s default territory.

Class of service
Select to assign the user a class of service, which determines the priority of the user’s calls.
If not selected, the user receives the highest class of service associated with any group to which the user belongs, or if none, the system’s default class of service. See Conference Settings.
Note: A class of service may also be assigned to an endpoint. The class of service of the device applies to point-to-point calls. VMR calls use the class of service of the conference room.

Maximum bit rate (kbps)
If Class of service is selected, lets you specify the maximum bit rate for the user.

Minimum downspeed rate (kbps)
If Class of service is selected, lets you specify the minimum bit rate to which the user’s calls can be reduced (downspeeded).

Associated Roles
Available roles
Lists the roles available to assign to the user. All users are automatically assigned the Conferencing User role, but it is not listed or explicitly assigned. Select the role or roles you want to assign.
Note: Explicitly assigned roles give the user access to the system’s management interface.

Conference Passcodes
Chairperson passcode
The numeric passcode that identifies chairpersons in the user’s conferences. If none, the user’s conferences don’t include the chairperson feature.
Must contain numeric characters only (the digits 0-9) and may be up to 16 digits long. Cannot be the same as the conference passcode.
The passcode can also be set individually for each of the user’s conference rooms.

Conference passcode
The numeric passcode that callers must enter to join the user’s conferences. If none, the user’s conferences do not require a passcode.
Must contain numeric characters only (the digits 0-9) and may be up to 16 digits long. Cannot be the same as the chairperson passcode.
The passcode can also be set individually for each of the user’s conference rooms.

4 Click OK.
**Edit a Local User**

For enterprise users, you can change their roles and their chairperson and conference passcodes, and you can enable or disable their accounts, but you cannot change user names, user IDs, or user passwords.

For local users, you can change everything but the user ID.

**Note:** If Cisco Codian MCUs are included in the Polycom RealPresence DMA system’s pool of conferencing resources, do not assign a chairperson passcode without also assigning a conference passcode. If a conference with only one passcode (either chairperson or conference) lands on a Codian MCU, all callers to the conference must enter that passcode.

**To edit a user:**

1. Go to **User > Users**.
2. Enter the search criteria you want and click **Search** to display users that match your criteria.
3. Select the user to edit.
4. Click **Edit** in the **Actions** list.
5. In the **Edit User** window, edit the fields as described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Info</strong></td>
<td></td>
</tr>
<tr>
<td>First name</td>
<td>The local user’s first name.</td>
</tr>
<tr>
<td>Last name</td>
<td>The local user’s last name.</td>
</tr>
<tr>
<td>User ID</td>
<td>The local user’s login name.</td>
</tr>
<tr>
<td><strong>Password Confirm password</strong></td>
<td>The local user’s system login password (not conference or chairperson passcode). This is the password that enables users with explicitly assigned roles to log into the system’s management interface. The password must satisfy the local password rules specified for the system.</td>
</tr>
<tr>
<td>Email address</td>
<td>The local user’s email address.</td>
</tr>
<tr>
<td>User pass-through to CDR</td>
<td>Optional value to put in the <strong>userDataA</strong> field of call detail records (CDRs) associated with this user. For example, this might be a user ID from some external system or database.</td>
</tr>
<tr>
<td>Account disabled</td>
<td>If selected, the user cannot host conferences (the user’s conference room or rooms are not available) and cannot access the system’s management interface. You can select the check box and still create the user account, but not activate it immediately.</td>
</tr>
</tbody>
</table>
### Conference room territory
The territory to which the user’s conference rooms (virtual meeting rooms, or VMRs) are assigned.
A conference room’s territory assignment determines which RealPresence DMA cluster hosts the room’s conferences (the primary cluster for the territory, or its backup cluster if necessary).
If not selected, the user’s conference rooms are assigned as follows (in priority order listed):
- To the territory associated with the room specifically.
- To the territory associated with the Active Directory group the user belongs to (if more than one, the group that is alphabetically first).
- To the system’s default territory.

### Class of service
Select to assign the user a class of service, which determines the priority of the user’s calls.
If not selected, the user receives the highest class of service associated with any group to which the user belongs, or if none, the system’s default class of service. See Conference Settings.
**Note:** A class of service may also be assigned to an endpoint. The class of service of the device applies to point-to-point calls. VMR calls use the class of service of the conference room.

### Maximum bit rate (kbps)
If Class of service is selected, lets you specify the maximum bit rate for the user.

### Minimum downspeed rate (kbps)
If Class of service is selected, lets you specify the minimum bit rate to which the user’s calls can be reduced (downspeeded).

### Associated Roles
**Available roles**
Lists the roles available to assign to the user. All users are automatically assigned the Conferencing User role, but it is not listed or explicitly assigned. Select the role or roles you want to assign.
**Note:** Explicitly assigned roles give the user access to the system’s management interface.

### Conference Passcodes
**Chairperson passcode**
The numeric passcode that identifies chairpersons in the user’s conferences. If none, the user’s conferences don’t include the chairperson feature.
Must contain numeric characters only (the digits 0-9) and may be up to 16 digits long. Cannot be the same as the conference passcode.
The passcode can also be set individually for each of the user’s conference rooms.

**Conference passcode**
The numeric passcode that callers must enter to join the user’s conferences. If none, the user’s conferences do not require a passcode.
Must contain numeric characters only (the digits 0-9) and may be up to 16 digits long. Cannot be the same as the chairperson passcode.
The passcode can also be set individually for each of the user’s conference rooms.

6  Click **OK**.

Polycom, Inc.  350
**Find a User**

You can search for specific local or enterprise users based on search strings, search filters, and wildcards (*). The system matches the exact string you enter against the user ID, first name, and last name. If you enter "sam," the system displays users whose IDs or first or last names are "sam," but the results will not include IDs, first, or last names of "samuels." To search for a user when you have only a partial user ID or name, you can use an asterisk (*) as a wildcard. For example, to find users with the user ID, first, or last name of "samuels," enter any of the following search strings:

- sa*
- sam*ls
- *ls

**To find a user:**

1. Go to User > Users.
2. For a simple search, enter a search string in the Search field and press ENTER.
3. For more search options, click the filter button to the right of the Search field.
4. Select the filters you want, enter search strings for one or more fields and click Search.

The system displays the users matching your search criteria. The results include the following information:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>The user’s login name. The icon to the left indicates whether the user’s account is enabled or disabled. Hover over it to see the associated message.</td>
</tr>
<tr>
<td>First Name</td>
<td>The user’s first name.</td>
</tr>
<tr>
<td>Last Name</td>
<td>The user’s last name.</td>
</tr>
<tr>
<td>Domain</td>
<td>The domain associated with the user. All users added manually to the system are in the LOCAL domain.</td>
</tr>
<tr>
<td>Class of Service</td>
<td>The class of service assigned to the user, which determines the priority of the user’s calls. <strong>Note:</strong> The class of service of the device applies to point-to-point calls. VMR calls use the class of service of the conference room.</td>
</tr>
<tr>
<td>Conference Rooms</td>
<td>The user’s conference room or rooms (virtual meeting rooms, or VMRs). If the system is integrated with an Active Directory, and you specified criteria for conference room ID generation, the enterprise users have a default conference room assigned to them automatically. Alternatively or in addition, enterprise users may have custom conference rooms manually assigned to them. Local users must be manually assigned a conference room or rooms.</td>
</tr>
<tr>
<td>Roles</td>
<td>The user’s explicitly assigned user roles. All users automatically have the Conferencing User role; it’s not listed or explicitly assigned (but a conference room ID is required).</td>
</tr>
</tbody>
</table>
The RealPresence DMA system’s user database is unsorted. To avoid performance issues, if your query matches more than 4000 users, the system does not attempt to sort the results.

Delete a Local User
You can delete local users from the system when necessary.

To delete a local user:
1. Go to **User > Users**.
2. If necessary, filter the **Users** list to find the user to be deleted.
   - You can only delete local users, not users added from the Active Directory.
3. Select the user to delete.
4. Under **Actions**, click **Delete**.
5. Click **Yes** to confirm the deletion.
   - The user is deleted from the Polycom RealPresence DMA system.

Change Your Local User Password
You can configure the system to expire local user passwords after a certain number of days (see Configure Local Password Settings). If your password has expired when you try to log into the system, the **Change Password** dialog prompts you for a new password.

You can change your password at other times, as well.

To change your password:
1. Click **admin** and select **Change Password**.
2. Complete the fields as described in the following table:
Conference Rooms

In the RealPresence DMA system, a user may have three types of conference rooms:

- One enterprise conference room (if this is an enterprise user) automatically assigned to the user as part of the Active Directory integration process. You cannot delete this conference room, but you can modify it.
- Custom conference rooms that you manually add.
- Calendared conference rooms created by the Polycom One Touch Dial App when a user schedules a conference in Microsoft Outlook 365. You can modify some of the settings for these conference rooms, but not the ones set in the Outlook meeting invitation.

In addition, if you have a Polycom RealPresence Resource Manager system connected to the RealPresence DMA system’s RealPresence Platform API, the RealPresence Resource Manager system can create two types of conference rooms (VMRs) in the RealPresence DMA system:

- Scheduled meeting conference rooms that are short-lived (they have a start and end time). These rooms belong to the Conferencing Users who set up the meetings in the RealPresence Resource Manager system’s scheduling interface.
- Preset dial-out conference rooms (called Anytime conferences in the RealPresence Resource Manager system), which can be used at any time by someone with the chairperson passcode to initiate a dial-out conference to a preset list of participants. These rooms belong to the user account for the RealPresence Resource Manager system.

View Conference Rooms

You can view a selected user’s conference rooms (virtual meeting rooms, or VMRs).

To view conference rooms:

1. Go to User > Users.
2. Enter the search criteria you want and click Search to display users that match your criteria.
3. Select the user with the conference rooms to view.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>The user name that you use to log in. Display only.</td>
</tr>
<tr>
<td>Old password</td>
<td>The password that you want to change.</td>
</tr>
<tr>
<td>New password</td>
<td>Enter a new password. The password must satisfy the local password rules specified for the system (see Configure Local Password Settings).</td>
</tr>
<tr>
<td>Confirm new password</td>
<td>Retype the new password.</td>
</tr>
</tbody>
</table>

3. Click OK.
4. Under Actions, click **Manage Conf Rooms**.

The following table describes the information that displays in the **Conference Rooms** list.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Room ID</td>
<td>The unique ID of the room. Icons identify enterprise conference rooms and calendared meeting (Polycom Conferencing for Outlook) conference rooms.</td>
</tr>
<tr>
<td>Dial-in #</td>
<td>Number used to dial into the conference room. Automatically set to the dialing prefix plus the room ID.</td>
</tr>
<tr>
<td>Room Aliases</td>
<td>The aliases of the conference room that can be dialed to join a conference.</td>
</tr>
<tr>
<td>Conference Template</td>
<td>The template used by the conference room, which defines the conference properties (or links to the Polycom MCU conference profile) used for its conferences. The template assignment can be made at the conference room level, AD group level, or system default level.</td>
</tr>
<tr>
<td>MCU Pool Order</td>
<td>MCU pool order used by this conference room, which is used to determine which MCU hosts a conference. The pool order assignment can be made at the conference room level, AD group level, or system default level.</td>
</tr>
<tr>
<td>Territory</td>
<td>The territory to which the conference room is assigned. A conference room’s territory assignment determines which RealPresence DMA cluster hosts the conference (the primary cluster for the territory, or its backup cluster if necessary). The assignment can be made at the conference room level, user level, AD group level, or system default level.</td>
</tr>
<tr>
<td>Max Participants</td>
<td>Maximum number of callers allowed to join the conference. <strong>Automatic</strong> means the MCU’s maximum is used.</td>
</tr>
<tr>
<td>Initial Start Time</td>
<td>For a conference room created by the Polycom RealPresence DMA system for a calendared meeting (Polycom Conferencing for Outlook), the start time and date of the meeting. For a conference room created by the Polycom RealPresence Resource Manager system (via the RealPresence DMA system API) for a non-Lync scheduled meeting, the start time and date of the meeting.</td>
</tr>
<tr>
<td>Expiration Time</td>
<td>For a conference room created by the Polycom RealPresence Resource Manager (via the RealPresence DMA system API) for a scheduled meeting, the end time and date of the meeting.</td>
</tr>
</tbody>
</table>

**Add a Conference Room for a User**

You can create a custom conference room for any user. For a local user, you must add at least one conference room to give the user conferencing access.

You can create additional custom conference rooms for a local or enterprise user to offer the user a different conferencing experience (for example, by assigning a different conference template to the room) or an alternate room ID and dial-in number.
To add a conference room for a user

1. Go to User > Users.
2. Enter the search criteria you want and click Search to display users that match your criteria.
3. Select the user for whom to add a conference room.
4. Under Actions, click Manage Conf Rooms.
5. In the Conference Rooms window, click Add.
6. In the Add Conference Room window, complete the fields described in the following table as required.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Settings</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Room ID             | The unique ID of the conference room. Enter a Room ID or click Generate to let the system pick a random available ID from the range set in Conference Settings. Valid Room IDs must meet the following requirements:  
  • Must start and end with an alphanumeric character.  
  • Characters in the middle may be alphanumeric or any of the following:  
    _ ~ ! $ & , . ' = + - * ( )  
    % is allowed only if it is followed by at least two alphanumeric characters.  
  • Cannot contain blank spaces. |
| Dial-in #           | Number used to dial into the conference room. Automatically set to the dialing prefix plus the room ID. |
| Conference template | The template used by the conference room, which defines the conference properties (or links to the Polycom MCU conference profile) used for its conferences. If not selected, the room uses the highest-priority template associated with any group to which the user belongs, or if none, the system’s default template. Caution: If this template is linked to a RealPresence Collaboration Server or RMX profile, the profile’s IVR service determines whether callers are prompted for passcodes:  
  • If the profile’s IVR service prompts for passcodes, callers are prompted even if the conference doesn’t have a passcode.  
  • If the profile’s IVR service doesn’t prompt for passcodes, callers aren’t prompted even if the conference has a conference or chairperson passcode. |
| Max participants    | Maximum number of callers allowed to join the conference. Automatic means the MCU’s maximum is used. If not selected, the room uses the system’s default maximum. |
| Chairperson required| If checked, the conference will only start when a chairperson joins the conference. The user or conference room should be configured with a chairperson passcode or chairperson alias. This setting applies even if Conference requires chairperson is not selected in the conference template.  
  Note: See Caution for the Conference Template field. |
Users

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Presence               | In a Lync 2013 or Skype for Business 2015 environment, you can configure presence publishing (the publishing of VMR status to a Skype client contact list) for each VMR. Enable this check box to override the system-wide default presence publishing settings defined in Conference Settings.

**Note**: This option is visible only if the Publish presence for Polycom conference contacts check box is selected in Conference Settings.

Depending on the settings of the Publish presence for Polycom conference contacts and Create Polycom conference contacts check boxes, there are two modes of operation for this field:

- When Publish presence for Polycom conference contacts is checked and Create Polycom conference contacts is unchecked, the following options display:
  - Publish presence
  - Do not publish presence

  These options control whether the RealPresence DMA system will publish presence status for this Polycom conference contact.

- When both Publish presence for Polycom conference contacts and Create Polycom conference contacts are checked, the following options display:
  - Create contact and publish presence
  - Do not create contact or publish presence

  These options control whether the RealPresence DMA system will create an Active Directory contact resource for and publish presence for this Polycom conference contact.

<table>
<thead>
<tr>
<th>Conference Duration</th>
<th>If selected, the maximum duration of a conference in Hours and Minutes, or Unlimited (the maximum in this case depends on the MCU). If not selected, the room uses the longest duration associated with any group to which the user belongs, or if none, the system’s default maximum duration. Duration overrides last disconnect – when checked, an active conference will not be terminated when all participants have left the conference but will continue until the conference duration is reached. This allows participants to join/rejoin the conference using the passcodes that are current for the conference. This is useful when the conference chairperson has changed the passcodes during the conference or when the conference room passcodes have changed during the conference. If not selected, participants dialing in would use the settings in the conference room. If selected, participants dialing in would use the settings current for the conference.</th>
</tr>
</thead>
</table>
| Territory            | The territory to which the conference room is assigned. A conference room’s territory assignment determines which RealPresence DMA cluster hosts its conferences (the primary cluster for the territory, or its backup cluster if necessary). If not selected, the conference room is assigned as follows (in priority order listed):
  - To the territory associated with the user.
  - To the territory associated with the AD group the user belongs to (if more than one, the lexically first group).
  - To the system’s default territory. |
### Field | Description
--- | ---
MCU pool order | MCU pool order used by this conference room to determine which MCU hosts a conference. If not selected, the room uses the highest-priority pool order associated with any group to which the user belongs, or if none, the system’s default pool order.

### MCU Selection
The method for the RealPresence DMA system to use when it selects MCUs from MCU pool orders:
- **Prefer MCU in first MCU pool** ensures that the DMA system always routes the call to the first available MCU in the first MCU pool. If no MCU is available, the system searches the second MCU pool for an available MCU, and so on.
- **Prefer MCU in first caller’s site** matches the MCU chosen for the call with the site that the first caller’s endpoint belongs to.

### Conference room pass-through to CDR
Optional value to put in the `userDataA` field of conference Call Detail Records (CDRs) associated with this user. For example, this might be a user ID from some external system or database.

### Passcodes and Aliases

#### Chairperson passcode
The numeric passcode that identifies chairpersons in this room’s conferences. If none, the room’s conferences do not include the chairperson feature. If the user has a chairperson passcode, it displays here. You can change it to a different passcode for this room only. Must contain numeric characters only (the digits 0-9) and may be up to 16 digits long. Cannot be the same as the conference passcode.

**Note:** See **Caution** for the **Conference Template** field.

**Use as Alias**
When checked, the RealPresence DMA system creates a Conference room alias from the Chairperson passcode and assigns Chairperson as the role for the alias. The alias and role display in the Conference Room Alias and Conference Role list.

**Note:** To change the Chairperson passcode, edit the **Chairperson passcode** field. Updated information displays in the Conference Room Alias list.

#### Conference passcode
The numeric passcode that participants must enter to join this room’s conferences. If none, the room’s conferences do not require a passcode. If the user has a conference passcode, it appears here. You can change it to a different passcode for this room only. Must contain numeric characters only (the digits 0-9) and may be up to 16 digits long. Cannot be the same as the chairperson passcode.

**Note:** See **Caution** for the **Conference Template** field.

**Use as Alias**
When checked, the RealPresence DMA system creates a Conference room alias from the Conference passcode and assigns Participant as the role for the alias. The alias and role display in the Conference Room Alias and Conference Role list.

**Note:** To change the Conference passcode, edit the Conference passcode field. Updated information displays in the Conference Room Alias list.

#### Conference room alias
The alias of the conference room that can be dialed to join a conference. Can contain alphanumeric and special characters. Cannot contain spaces.
### Conference role

The specific conference role associated with the conference room alias. If the role assigned to the Conference room alias is **Role determined by passcode entry (when defined)**, then the caller is prompted for a passcode when they dial the conference room alias. If the caller enters the chairperson passcode, they enter the conference as a chairperson.

If the **Chairperson** conference role has been assigned to the conference alias, the caller joins the conference as a chairperson, without being prompted for the chairperson passcode.

### Preset Dialouts

**Presets Dialouts**

If enabled, this conference room is for a **preset dialout** conference, referred to in the Polycom RealPresence Resource Manager system as an **Anytime** conference. When someone dials in and starts a conference, the RealPresence DMA system dials out to the entries in the **Preset Dialout Participants** list.

Note that for the RealPresence DMA system to dial out from an H.323 conference, the Polycom RealPresence Collaboration Server (MCU) hosting the conference must be H.323 registered to one of the RealPresence DMA clusters in the supercluster.

The system does not forward dialouts to endpoints with call forwarding activated.

Disabling Preset Dialouts lets you turn off the automatic dialout temporarily without losing the configuration data.

To prevent unauthorized persons from being able to trigger the dialout, do the following:

- Set **Conference template** to a template that requires a chairperson to start the conference.
- Specify a chairperson passcode for this conference room or this user.

**Note:** If the conference template in use requires a chairperson, the dialout does not occur until the first chairperson has joined, regardless of the number of other participants in the conference. Similarly, if the conference includes a conference passcode, the dial-out will not occur until a participant enters the passcode successfully.

**Preset Dialout Participants**

Lists the names and URIs of the participants to be automatically dialed when the conference starts.

**Note:** If an icon appears in the **Settings** column for a participant, hover your mouse cursor over the icon for more information.

### Scheduling and Integration

**Initial start time**

The start time of a single conference or the start time for the first meeting in a recurring series.

**Expiration time**

The end time of a single conference or the end time for the last meeting in a recurring series.

**Conference focus URI**

The sip URI that identifies the Skype for Business conference to which this VMR will be connected. As part of the Polycom RealConnect™ solution for Microsoft Office365, the One Touch Dial App will populate this value from Office365 calendared meetings. For other Skype for Business deployments, this value may be obtained from the Skype system.
Users

Edit a Conference Room for a User

You can revise a conference room’s details as needed.

To edit a conference room for a user:

1. Go to User > Users.
2. Enter the search criteria you want and click Search to display users that match your criteria.
3. Select the user with the conference room to edit.
4. Under Actions, click Manage Conf Rooms.
5. In the Conference Rooms window, select a conference room from the list and click Edit.

7. Click OK.

Field | Description
---|---
Destination network | Host name, FQDN, or network domain label, with or without port and URL parameters, of the Microsoft federated environment (Lync, Skype for Business, or Office 365) that is hosting the conference. This field is required when the Microsoft environment is federated and the focus URI does not provide a correct destination network. It can be left blank if the Microsoft environment is not federated.

**Note:** For Microsoft Office365 conferences, the Polycom® One Touch Dial App will populate this value from Office 365 calendared meetings. For other Skype for Business deployments, this value may be obtained from the Skype system.

**AS-SIP Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource priority namespace</td>
<td>In an Assured Services SIP (AS-SIP) environment, a Local Session Controller (LSC) can provide priority-based precedence and preemption services to ensure that the most important calls get through. If your organization has implemented such a resource prioritization mechanism and you want to assign this conference room a priority value different from the system’s default, set this field to the namespace being used for resource priority values. If the namespace being used is not listed, select Custom and enter the name in the box below the list.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Resource priority value | If the RealPresence DMA system is deployed in an AS-SIP environment with a resource prioritization mechanism and Local Session Controller (LSC), set this to the priority value to assign to conferences using this conference room. If using a custom namespace, enter the value in the box below the list. The string namespace:value is used in the SIP Resource-Priority header of outbound calls from this conference room and recorded in the conference property changes. For inbound calls to this conference room:

• If the INVITE message contains a resource priority value, the RealPresence DMA system passes that value to the MCU.

• If the INVITE message doesn’t contain a resource priority value, the RealPresence DMA system provides the value assigned here to the MCU on behalf of the endpoint. In either case, the resource priority value is recorded in the call property changes. |
6 In the **Edit Conference Room** window, revise the fields described in the following table as needed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Settings</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Room ID             | The unique ID of the conference room. Enter a Room ID or click **Generate** to let the system pick a random available ID from the range set in Conference Settings. Room IDs must meet the following requirements in order to be valid:  
  - Must start and end with an alphanumeric character.  
  - Characters in the middle may be alphanumeric or any of the following: _ ~ ! $ & , . ' = + * ( )  
  - % is allowed only if it is followed by at least two alphanumeric characters.  
  - Cannot contain blank spaces. |
| Dial-in #           | Number used to dial into the conference room. Automatically set to the dialing prefix plus the room ID. |
| Conference template | The template used by the conference room, which defines the conference properties (or links to the Polycom MCU conference profile) used for its conferences. If not selected, the room uses the highest-priority template associated with any group to which the user belongs, or if none, the system’s default template. **Caution:** If this template is linked to a RealPresence Collaboration Server or RMX profile, the profile’s IVR service determines whether callers are prompted for passcodes:  
  - If the profile’s IVR service prompts for passcodes, callers are prompted even if the conference doesn’t have a passcode.  
  - If the profile’s IVR service doesn’t prompt for passcodes, callers aren’t prompted even if the conference has a conference or chairperson passcode. |
| Max participants    | Maximum number of callers allowed to join the conference. **Automatic** means the MCU’s maximum is used. If not selected, the room uses the system’s default maximum. |
| Chairperson required| If checked, the conference will only start when a chairperson joins the conference. The user or conference room should be configured with a chairperson passcode or chairperson alias. This setting applies even if **Conference requires chairperson** is not selected in the conference template. **Note:** See **Caution** for the **Conference Template** field. |
In a Lync 2013 or Skype for Business 2015 environment, you can configure presence publishing (the publishing of VMR status to a Skype client contact list) for each VMR. Enable this check box to override the system-wide default presence publishing settings defined in Conference Settings.

**Note:** This option is visible only if the Publish presence for Polycom conference contacts check box is selected in Conference Settings.

Depending on the settings of the Publish presence for Polycom conference contacts and Create Polycom conference contacts check boxes, there are two modes of operation for this field:

- When Publish presence for Polycom conference contacts is checked and Create Polycom conference contacts is unchecked, the following options display:
  - Publish presence
  - Do not publish presence

  These options control whether the RealPresence DMA system will publish presence status for this Polycom conference contact.

- When both Publish presence for Polycom conference contacts and Create Polycom conference contacts are checked, the following options display:
  - Create contact and publish presence
  - Do not create contact or publish presence

  These options control whether the RealPresence DMA system will create an Active Directory contact resource for and publish presence for this Polycom conference contact.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Presence</td>
<td>In a Lync 2013 or Skype for Business 2015 environment, you can configure presence publishing (the publishing of VMR status to a Skype client contact list) for each VMR. Enable this check box to override the system-wide default presence publishing settings defined in Conference Settings. <strong>Note:</strong> This option is visible only if the Publish presence for Polycom conference contacts check box is selected in Conference Settings. Depending on the settings of the Publish presence for Polycom conference contacts and Create Polycom conference contacts check boxes, there are two modes of operation for this field: - When Publish presence for Polycom conference contacts is checked and Create Polycom conference contacts is unchecked, the following options display:  - Publish presence  - Do not publish presence  These options control whether the RealPresence DMA system will publish presence status for this Polycom conference contact. - When both Publish presence for Polycom conference contacts and Create Polycom conference contacts are checked, the following options display:  - Create contact and publish presence  - Do not create contact or publish presence  These options control whether the RealPresence DMA system will create an Active Directory contact resource for and publish presence for this Polycom conference contact.</td>
</tr>
<tr>
<td>Conference Duration</td>
<td>If selected, the maximum duration of a conference in Hours and Minutes, or Unlimited (the maximum in this case depends on the MCU). If not selected, the room uses the longest duration associated with any group to which the user belongs, or if none, the system’s default maximum duration. <strong>Duration overrides last disconnect</strong> – when checked, an active conference will not be terminated when all participants have left the conference but will continue until the conference duration is reached. This allows participants to join/rejoin the conference using the passcodes that are current for the conference. This is useful when the conference chairperson has changed the passcodes during the conference or when the conference room passcodes have changed during the conference. If not selected, participants dialing in would use the settings in the conference room. If selected, participants dialing in would use the settings current for the conference.</td>
</tr>
<tr>
<td>Territory</td>
<td>The territory to which the conference room is assigned. A conference room’s territory assignment determines which RealPresence DMA cluster hosts its conferences (the primary cluster for the territory, or its backup cluster if necessary). If not selected, the conference room is assigned as follows (in priority order listed):  - To the territory associated with the user.  - To the territory associated with the AD group the user belongs to (if more than one, the lexically first group).  - To the system’s default territory.</td>
</tr>
</tbody>
</table>
### Field

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCU pool order used by this conference room to determine which MCU hosts a conference. If not selected, the room uses the highest-priority pool order associated with any group to which the user belongs, or if none, the system’s default pool order.</td>
</tr>
<tr>
<td>The method for the RealPresence DMA system to use when it selects MCUs from MCU pool orders:</td>
</tr>
<tr>
<td>Prefer MCU in first MCU pool ensures that the DMA system always routes the call to the first available MCU in the first MCU pool. If no MCU is available, the system searches the second MCU pool for an available MCU, and so on.</td>
</tr>
<tr>
<td>Prefer MCU in first caller’s site matches the MCU chosen for the call with the site that the first caller’s endpoint belongs to.</td>
</tr>
<tr>
<td>Optional value to put in the userDataA field of conference Call Detail Records (CDRs) associated with this user. For example, this might be a user ID from some external system or database.</td>
</tr>
</tbody>
</table>

### Passcodes and Aliases

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chairperson passcode</td>
<td>The numeric passcode that identifies chairpersons in this room’s conferences. If none, the room’s conferences do not include the chairperson feature. If the user has a chairperson passcode, it displays here. You can change it to a different passcode for this room only. Must contain numeric characters only (the digits 0-9) and may be up to 16 digits long. Cannot be the same as the conference passcode.</td>
</tr>
<tr>
<td>Use as Alias</td>
<td>When checked, the RealPresence DMA system creates a Conference room alias from the Chairperson passcode and assigns Chairperson as the role for the alias. The alias and role display in the Conference Room Alias and Conference Role list.</td>
</tr>
<tr>
<td>Conference passcode</td>
<td>The numeric passcode that participants must enter to join this room’s conferences. If none, the room’s conferences do not require a passcode. If the user has a conference passcode, it appears here. You can change it to a different passcode for this room only. Must contain numeric characters only (the digits 0-9) and may be up to 16 digits long. Cannot be the same as the chairperson passcode.</td>
</tr>
<tr>
<td>Use as Alias</td>
<td>When checked, the RealPresence DMA system creates a Conference room alias from the Conference passcode and assigns Participant as the role for the alias. The alias and role display in the Conference Room Alias and Conference Role list.</td>
</tr>
<tr>
<td>Conference room alias</td>
<td>The alias of the conference room that can be dialed to join a conference. Can contain alphanumeric and special characters. Cannot contain spaces.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Conference role</td>
<td>The specific conference role associated with the conference room alias. If the role assigned to the Conference room alias is <strong>Role determined by passcode entry (when defined)</strong>, then the caller is prompted for a passcode when they dial the conference room alias. If the caller enters the chairperson passcode, they enter the conference as a chairperson.</td>
</tr>
<tr>
<td></td>
<td>If the Chairperson conference role has been assigned to the conference alias, the caller joins the conference as a chairperson, without being prompted for the chairperson passcode.</td>
</tr>
<tr>
<td>Preset Dialouts</td>
<td><strong>Presets Dialouts</strong> If enabled, this conference room is for a preset dialout conference, referred to in the Polycom RealPresence Resource Manager system as an <strong>Anytime</strong> conference. When someone dials in and starts a conference, the RealPresence DMA system dials out to the entries in the <strong>Preset Dialout Participants</strong> list. Note that for the RealPresence DMA system to dial out from an H.323 conference, the Polycom RealPresence Collaboration Server (MCU) hosting the conference must be H.323 registered to one of the RealPresence DMA clusters in the supercluster. The system does not forward dialouts to endpoints with call forwarding activated. Disabling Preset Dialouts lets you turn off the automatic dialout temporarily without losing the configuration data. To prevent unauthorized persons from being able to trigger the dialout, do the following:</td>
</tr>
<tr>
<td></td>
<td>• Set <strong>Conference template</strong> to a template that requires a chairperson to start the conference.</td>
</tr>
<tr>
<td></td>
<td>• Specify a chairperson passcode for this conference room or this user.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If the conference template in use requires a chairperson, the dialout does not occur until the first chairperson has joined, regardless of the number of other participants in the conference. Similarly, if the conference includes a conference passcode, the dial-out will not occur until a participant enters the passcode successfully.</td>
</tr>
<tr>
<td>Preset Dialout Participants</td>
<td>Lists the names and URIs of the participants to be automatically dialed when the conference starts.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If an icon appears in the <strong>Settings</strong> column for a participant, hover your mouse cursor over the icon for more information.</td>
</tr>
<tr>
<td>Scheduling and Integration</td>
<td><strong>Initial start time</strong> The start time of a single conference or the start time for the first meeting in a recurring series.</td>
</tr>
<tr>
<td></td>
<td><strong>Expiration time</strong> The end time of a single conference or the end time for the last meeting in a recurring series.</td>
</tr>
<tr>
<td></td>
<td><strong>Conference focus URI</strong> The sip URI that identifies the Skype for Business conference to which this VMR will be connected. As part of the Polycom RealConnect™ solution for Microsoft Office365, the One Touch Dial App will populate this value from Office365 calendared meetings. For other Skype for Business deployments, this value may be obtained from the Skype system.</td>
</tr>
</tbody>
</table>

Polycom, Inc.
Delete a Conference Room for a User

You can delete custom conference rooms for a user that you added manually in the RealPresence DMA system or via the API.

You cannot delete enterprise conference rooms, calendared meeting conference rooms (Polycom Conferencing for Outlook), or scheduled conference rooms created by the Polycom RealPresence Resource Manager system via the API.

To delete a conference room for a user

1. Go to User > Users.
2. Select the user with the custom conference room you want to delete.

7. Click OK.
3 Under Actions, click Manage Conf Rooms.
4 In the Conference Rooms window, select the conference room to delete and click Delete.
5 Click Yes to delete the selected conference room.

Add a Conference Room Alias and Conference Role

An alias is an alternative way to dial to join a conference. When a caller dials in to a conference using an alias, they join the conference with the conference role associated with that alias. For example, if the conference alias has been assigned the chairperson conference role, the caller joins the conference as a chairperson, without being prompted for the chairperson passcode.

In the RealPresence DMA system, you can define aliases for a conference room and associate a conference role with each alias.

To add a new conference room alias and conference role
1 Go to User > Users.
2 Enter the search criteria you want and click Search to display users that match your criteria.
3 Select the user for whom to add the conference room alias and conference role.
4 Under Actions, click Manage Conf Rooms.
5 Select an existing conference room from the list and click Edit, or Add a new one.
6 In the Add Conference Room or Edit Conference Room window, select the Passcodes and Aliases section.
7 Click Add.
8 In the Add Conference Room Alias window, do one of the following:
   a Click Generate to automatically create an alias for the conference room.
   b Enter an alias of your own choosing.
9 Under Conference Role, select the role to associate with the conference room alias.
10 Click OK.

Edit a Conference Room Alias and Conference Role

In the RealPresence DMA system, you can revise or generate a new alias for a conference room and change the conference role associated with an alias. Note that it is not required to change both a conference room alias and its conference role.

To edit a conference room alias and conference role
1 Go to User > Users.
2 Enter the search criteria you want and click Search to display users that match your criteria.
3 Select the user with the conference room alias or conference role to edit.
4 Under Actions, click Manage Conf Rooms.
5 Select an existing conference room from the list and click Edit.
6 In the Edit Conference Room window, select the Passcodes and Aliases section.
7 Select a Conference Room Alias and click Edit.
8 In the Edit Conference Room Alias window, click Generate or enter a new value if you want to create a new alias for the conference room.
9 Under Conference Role, choose a new role to associate with the conference room alias, if desired.
10 Click OK.

**Delete a Conference Room Alias and Conference Role**

You can delete a conference room alias and its associated role from the RealPresence DMA system as needed.

**To delete a conference room alias and conference role**
1 Go to User > Users.
2 Enter the search criteria you want and click Search to display users that match your criteria.
3 Select the user to delete.
4 Under Actions, click Manage Conf Rooms.
5 Select an existing conference room from the list and click Edit.
6 In the Edit Conference Room window, select the Passcodes and Aliases section.
7 Select a Conference Room Alias and click Delete.
8 Click Yes to confirm the deletion.

**Add a Dialout Participant**

You can add a conference participant to a conference room’s Preset Dialout Participants list. When someone dials into the conference room and starts a conference, the RealPresence DMA system dials out to the participants in the list.

**To add a dial-out participant**
1 Go to User > Users.
2 Enter the search criteria you want and click Search to display users that match your criteria.
3 Select the user to add to the Preset Dialout Participants list.
4 Under Actions, click Manage Conf Rooms.
5 Select an existing conference room from the list and click Edit, or add a new one.
6 In the Add Conference Room or Edit Conference Room window, select Preset Dialouts.
7 Select the Enabled check box.
8 Click Add.
In the **Add Dialout Participant** window, complete the fields as described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participant name</td>
<td>The name of the participant.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The protocol used to dial the participant (SIP, H.323, ISDN).</td>
</tr>
<tr>
<td>Dial-out URI</td>
<td>Dial string used to dial the participant. If you select SIP or ISDN as the</td>
</tr>
<tr>
<td></td>
<td><strong>Protocol</strong>, the system adds a schema (i.e., sip: or isdn:) before the URI.</td>
</tr>
<tr>
<td>Extension</td>
<td>You can specify optional extension digits for ISDN dial-out connections. The</td>
</tr>
<tr>
<td></td>
<td>characters '#' and 'p' are allowed.</td>
</tr>
<tr>
<td>Connection encryption</td>
<td>Available for H.323 and ISDN connections only.</td>
</tr>
<tr>
<td></td>
<td>If enabled, the system instructs the MCU to encrypt this participant's connection.</td>
</tr>
<tr>
<td>Line rate</td>
<td>Select <strong>Automatic</strong> or select the specific <strong>Rate (kbps)</strong> to use for dial-out calls to the participant.</td>
</tr>
<tr>
<td>Audio-only</td>
<td>Available for H.323 and ISDN connections only.</td>
</tr>
<tr>
<td></td>
<td>If enabled, the system instructs the MCU to use an audio-only connection for this participant.</td>
</tr>
<tr>
<td>Auto disconnect</td>
<td>Available for H.323 and ISDN connections only.</td>
</tr>
<tr>
<td></td>
<td>Any dial-out participants you mark as Auto-disconnect are automatically disconnected once they are the only participants left in the conference. After they are disconnected, the conference ends.</td>
</tr>
<tr>
<td></td>
<td>You can use this feature to prevent MCU-to-MCU dial-outs from remaining open after the conference has ended.</td>
</tr>
</tbody>
</table>

10. Click **OK**.

**Edit a Dialout Participant**

You can edit a participant in a conference room's **Preset Dialout Participants** list, changing the name or dial string for the participant. The RealPresence DMA system dials out to the participants in the list.

**To edit a dial-out participant:**

1. Go to **User > Users**.
2. Enter the search criteria you want and click **Search** to display users that match your criteria.
3. Select the user to edit.
4. Under **Actions**, click **Manage Conf Rooms**.
5. Select an existing conference room from the list and click **Edit**.
6. In the **Edit Conference Room** window, select the **Preset Dialouts** section.
7. Ensure the **Enabled** check box is checked.
8. Select a dial-out participant from the list.
9. Click **Edit**.
In the **Edit Dialout Participant** window, edit the following fields as required:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participant name</td>
<td>The name of the participant.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The protocol used to dial the participant (SIP, H.323, ISDN).</td>
</tr>
<tr>
<td>Dial-out URI</td>
<td>Dial string used to dial the participant. If you select SIP or ISDN as the Protocol, the system adds a schema (i.e., sip: or isdn:) before the URI.</td>
</tr>
<tr>
<td>Extension</td>
<td>You can specify optional extension digits for ISDN dial-out connections. The characters '#' and 'p' are allowed.</td>
</tr>
<tr>
<td>Connection encryption</td>
<td>Available for H.323 and ISDN connections only. If enabled, the system instructs the MCU to encrypt this participant's connection.</td>
</tr>
<tr>
<td>Line rate</td>
<td>Select <strong>Automatic</strong> or select the specific <strong>Rate (kbps)</strong> to use for dial-out calls to the participant.</td>
</tr>
<tr>
<td>Audio-only</td>
<td>Available for H.323 and ISDN connections only. If enabled, the system instructs the MCU to use an audio-only connection for this participant.</td>
</tr>
<tr>
<td>Auto disconnect</td>
<td>Available for H.323 and ISDN connections only. Any dial-out participants you mark as Auto-disconnect are automatically disconnected once they are the only participants left in the conference. After they are disconnected, the conference ends. You can use this feature to prevent MCU-to-MCU dial-outs from remaining open after the conference has ended.</td>
</tr>
</tbody>
</table>

Click **OK**.

**Delete a Dial-out Participant**

You can delete a participant in a conference room's **Preset Dialout Participants** list when necessary.

**To delete a dial-out participant:**

1. Go to **User > Users**.
2. Enter the search criteria you want and click **Search** to display users that match your criteria.
3. Select the user to delete.
4. Under **Actions**, click **Manage Conf Rooms**.
5. Select an existing conference room from the list and click **Edit**.
6. In the **Edit Conference Room** window, select the **Preset Dialouts** section.
7. Ensure the **Enabled** check box is checked.
8. Select the dial-out participant to delete from the list.
9. Click **Delete**.
Associated Endpoints

Users can be associated with or disassociated from specific endpoints. You can also manage user-to-device associations on the Endpoints page.

**Associate a User With a Device**

You can associate a user with an endpoint by selecting the user, then searching for the endpoint to associate with the user. You can search by device **Alias**, **IP Address**, **Name**, **Model**, **Owner**, **Owner domain** or a combination of these criteria.

The system matches the search string you enter against the beginning of the field you are searching. For example, if you enter "sa" in the endpoint **Name** field, the search results display endpoints with names that begin with "sa." To search for a matching string not at the beginning of the field, you can use an asterisk (*) as a wildcard, such as "*sa".

**To associate a user with a device:**

1. Go to **User > Users**.
2. Enter the search criteria you want and click **Search** to display users that match your criteria.
3. Select the user to associate with an endpoint.
4. Under **Actions**, click **Manage Associated Endpoints**.
   - The **Associated Endpoints** window displays the endpoints associated with the user, if any.
5. Click **Add**.
6. In the **Select Associated Endpoints** window, search for endpoints based on the criteria you enter.
7. Select one or more endpoints to associate with the user.
   - Use **SHIFT-CLICK** or **CTRL-CLICK** to select multiple endpoints.
8. Click **OK**, then click **OK** again.

**Disassociate a User From a Device**

You can disassociate a user from an endpoint by selecting the user, then deleting the association. Note that deleting the association does not delete the endpoint.

**To disassociate a user from a device:**

1. Go to **User > Users**.
2. Enter the search criteria you want and click **Search** to display users that match your criteria.
3. Select the user to disassociate from an endpoint.
4. Under **Actions**, click **Manage Associated Endpoints**.
   - The **Associated Endpoints** window displays the endpoints associated with the user.
5. Select one or more endpoints to disassociate and click **Delete**.
6. Click **Yes** to confirm the disassociation.
If you have integrated your RealPresence DMA system with a Microsoft® Active Directory (AD), you can assign roles and conference templates associated with user groups after you have imported the groups you want to use.

Groups functionality is available only if your Polycom RealPresence DMA system is integrated with an Active Directory. User groups are defined in your Active Directory and imported into the Polycom RealPresence DMA system.

You must be an enterprise user (with the appropriate user role assignments) to see and work with enterprise users. A local user can only see other local users, regardless of user roles.

Microsoft Active Directory provides two group types and four group scopes. The Polycom RealPresence DMA system supports only security groups (not distribution groups) with universal or global scope.

View Groups

The Groups page provides information about enterprise groups.

To view groups:

» Go to User > Groups.

The following table describes the fields on the Groups page:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>Name of the group, as defined in the Active Directory.</td>
</tr>
<tr>
<td>Description</td>
<td>Description from the Active Directory.</td>
</tr>
<tr>
<td>Domain</td>
<td>Name of the domain to which the group belongs.</td>
</tr>
</tbody>
</table>
| Class of service       | Class of service assigned to the group, which determines the priority of the group’s calls. If none, the group receives the system’s default class of service defined in Conference Settings. 
                         | **Note:** A class of service may also be assigned to a user or an endpoint.                                                      |
|                         | **Note:** The class of service of the device applies to point-to-point calls. VMR calls use the class of service of the conference room. |
Working with Enterprise Groups

You can customize the conferencing experience for members of an Active Directory group by assigning it a conference template. In addition, you can set RealPresence DMA user roles on a group basis which allows you to manage RealPresence DMA administrative access according to groups.

You must be logged in to the RealPresence DMA system as an enterprise user with the Administrator role to perform these procedures.

Import Enterprise Groups

After you have integrated your RealPresence DMA system with Active Directory, you can import enterprise groups to the RealPresence DMA system.

To import enterprise groups:
1. Go to User > Groups.
2. Under Actions, click Import Enterprise Groups.
3. Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conference Template</td>
<td>Template assigned to the group that defines the conference properties (or links to the Polycom MCU conference profile) used for the group’s conferences. You can assign a template at the conference room, AD group, or system default level.</td>
</tr>
<tr>
<td>MCU Pool Order</td>
<td>MCU pool order assigned to this group that is used to determine which MCU hosts a conference. You can assign the pool order assignment at the conference room, AD group, or system default level.</td>
</tr>
<tr>
<td>Territory</td>
<td>Territory to which the group’s conference rooms (virtual meeting rooms, or VMRs) are assigned. A conference room’s territory assignment determines which RealPresence DMA cluster hosts the conference (the primary cluster for the territory, or its backup cluster if necessary). You can assign a territory at the conference room level, the user level, the AD group level, or the system default level.</td>
</tr>
<tr>
<td>Assigned Roles</td>
<td>RealPresence DMA system roles, if any, that are automatically assigned to members of this group (all users automatically have the Conferencing User role; it’s not listed or explicitly assigned).</td>
</tr>
</tbody>
</table>
To set up an enterprise group:

1. In your Active Directory, create a security group containing the users to whom you want to give access to the RealPresence DMA system’s management user interface.
   
   You can assign all the user roles to a single group or create separate groups for each user role.

2. In the RealPresence DMA system, go to User > Groups.


4. Use Search to find the security group you created.

5. Move the group to the Groups to import box and click OK.

6. On the Groups page, select your new group.

7. Under Actions, click Edit.

8. Move the user roles you want to give members of this group to the Selected roles box.

9. Click OK.
   
   All members of this group will now share the system access privileges you assigned to the group.

10. To grant RealPresence DMA system access privileges to a user or remove those privileges, add or remove the user from the appropriate enterprise group.
Assign Conference Properties to a Group

You can assign the group a class of service, a template, an MCU pool, and more.

To edit a group:

1. Go to User > Groups.
2. Select the group of interest and click Edit.
3. Complete the following fields as needed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class of service</td>
<td>Select to assign the group a class of service other than the system’s default (see Conference Settings).</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The class of service of the device applies to point to point calls. VMR calls use the class of service of the conference room.</td>
</tr>
<tr>
<td>Maximum bit rate (kbps)</td>
<td>If Class of service is selected, specifies the maximum bit rate for the group.</td>
</tr>
<tr>
<td>Minimum downspeed bit rate (kbps)</td>
<td>If Class of service is selected, specifies the minimum bit rate to which the group’s calls can be reduced (downspeeded).</td>
</tr>
<tr>
<td>Conference template</td>
<td>Select to assign a template other than the system’s default (see Conference Settings). The template assignment can be made at the conference room level, AD group level, or system default level. It defines the conference properties (or links to the Polycom MCU conference profile) used for its conferences. See Conference Templates.</td>
</tr>
<tr>
<td>MCU pool order</td>
<td>Select to assign the group an MCU pool order other than the system’s default (see Conference Settings). The pool order assignment can be made at the conference room level, AD group level, or system default level. It’s used to determine which MCU hosts a conference. See MCU Pools and Pool Orders.</td>
</tr>
<tr>
<td>Territory</td>
<td>Select to assign the group’s conference rooms to a territory other than the system’s default (see Conference Settings). A conference room's territory assignment determines which RealPresence DMA cluster hosts the conference (the primary cluster for the territory, or its backup cluster if necessary). The assignment can be made at the conference room level, user level, AD group level, or system default level. <strong>Note:</strong> If a user belongs to more than one group, that user’s territory setting is inherited from the lexically first group (but does not change if the group is renamed). To be certain that a specific user’s conference rooms are assigned to a specific territory, assign that territory directly to the user. See Edit a Local User.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Presence publishing options                | In a Microsoft® Lync 2013 environment, you can configure presence publishing (the publishing of VMR status to a Lync 2013 client contact list) for any VMR that belongs to a member of this group. Enable this check box to override the system-wide default presence publishing settings defined on the [Service Config > Conference Manager Settings > Conference Settings](#) page.  
**Note:** This property is visible only if the [Publish presence for Polycom conference contacts](#) check box is enabled on the [Service Config > Conference Manager Settings > Conference Settings](#) page.  
**Note:** This property can be overridden on a per-VMR basis by the [Presence setting](#) on the [User > Users > Manage Conf Rooms](#) dialog.  
Depending on the settings of the [Publish presence for Polycom conference contacts](#) and [Create Polycom conference contacts](#) check boxes on the [Service Config > Conference Manager Settings > Conference Settings](#) page, there are two modes of operation for this field:  
• When [Publish presence for Polycom conference contacts](#) is checked and [Create Polycom conference contacts](#) is unchecked, the following options are displayed:  
  ▶ Publish presence  
  ▶ Do not publish presence  
  These options control whether the RealPresence DMA system will publish presence status for VMRs belonging to members of this group.  
• When both [Publish presence for Polycom conference contacts](#) and [Create Polycom conference contacts](#) are checked, the following options are displayed:  
  ▶ Create contact and publish presence  
  ▶ Do not create contact or publish presence  
  These options control whether the RealPresence DMA system will create an Active Directory contact resource for and publish presence for VMRs that belong to members of this group. |
| Default Conference Duration                 | Select to specify a maximum conference duration other than the system’s default (see [Conference Settings](#)). If you select **Unlimited**, the maximum depends on the MCU.                                                                 |
| Available roles                             | Lists the RealPresence DMA system roles available for automatic assignment to members of this group (all users automatically have the Conferencing User role; it’s not listed or explicitly assigned). See [User Roles](#).  
Use the arrows to move roles from the [Available roles](#) box to the [Selected roles](#) box or vice versa. |
| Selected roles                              | Lists the roles you’ve selected for members of this group.  
Remember, ordinary Conferencing Users have no explicitly assigned role. |

4 Click **OK**.

**Assign an MCU Pool Order to a Group**

You can specify which MCUs a group uses by assigning an MCU pool order to the group.
To assign an MCU pool order to a group:

1. If necessary, create the MCU pool and the pool order needed.
2. Go to User > Groups.
3. Select the group to which to assign the pool order.
5. In the MCU pool order list, select the pool order to be used for this group.
6. Click OK.

Assign a Conference Template to a Group

You can set up a custom conferencing experience for an enterprise group by assigning a conference template to that group.

To assign a conference template to an enterprise group:

1. Go to Service Config > Conference Manager Settings > Conference Templates and create a template that defines the conferencing experience for this group.
2. Optionally, under Actions, click Move Up until your new conference template has Priority 1. This ensures that users who have access to multiple conference templates will use this one for their enterprise conference room. You can choose a different priority level, but then some members of the group for which you created the template may use a higher-ranking template.
3. Go to User > Groups.
4. Select the group for which you created the template.
5. Under Actions, click Edit.
6. Select the template you created for this group.
7. Click OK.
Login Policy Settings

Login Policy Settings enable you to configure some security aspects of user access to the Polycom® RealPresence® DMA® system.

- Configure Local User Account Settings
- Configure Local Password Settings
- Configure Session Settings
- Configure Banner Settings
- Management Access Settings

Configure Local User Account Settings

From the Local User Account page, you can perform the following actions:

- Lock out users who have exceeded the specified number and frequency of login failures. The system locks the account either indefinitely or for the length of time you specify.
- Disable accounts that have been inactive a specified number of days.

To configure local user account settings

1. Go to User > Login Policy Settings > Local User Account.
2. Complete the fields in the following table as needed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Account Lockout</strong></td>
<td></td>
</tr>
<tr>
<td>Enable account lockout</td>
<td>Turns on lockout feature and enables lockout configuration fields below.</td>
</tr>
<tr>
<td>Failed login threshold</td>
<td>Specify how many consecutive login failures cause the system to lock an account.</td>
</tr>
<tr>
<td>Failed login window (hours)</td>
<td>Specify the time span within which the consecutive failures must occur in order to lock the account.</td>
</tr>
<tr>
<td>Customize user account lockout duration (minutes)</td>
<td>If selected, specify how long the user’s account remains locked. If not selected, the lockout is indefinite, and a user with a locked account must contact an Administrator to unlock it.</td>
</tr>
<tr>
<td><strong>Account Inactivity</strong></td>
<td></td>
</tr>
<tr>
<td>Customize account inactivity threshold (days)</td>
<td>Turns on disabling of inactive accounts and lets you specify the inactivity threshold that triggers disabling.</td>
</tr>
</tbody>
</table>
3 Click **Update** to save your settings.

### Configure Local Password Settings

From the **Local Password** page, you can specify age, length, and complexity requirements for the passwords of local administrator, auditor, and provisioner users. These rules do not apply to conferencing users’ conference and chairperson passcodes, or to Active Directory users.

**To configure local password settings**

1. Go to **User > Login Policy Settings > Local Password**.
2. Complete the fields in the following table as needed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Password Management</strong></td>
<td></td>
</tr>
<tr>
<td>Maximum password age (days)</td>
<td>The age at which a password expires (30-180 days).</td>
</tr>
<tr>
<td>Minimum password age (days)</td>
<td>Specifies how frequently a password can be changed (1-30 days).</td>
</tr>
<tr>
<td>Minimum length</td>
<td>The number of characters a password must contain (1-30).</td>
</tr>
<tr>
<td>Minimum changed characters</td>
<td>The number of characters that must be different from the previous password (1-4).</td>
</tr>
<tr>
<td>Reject previous passwords</td>
<td>Specifies how many of the user’s previous passwords the system remembers and cannot be reused (8-16).</td>
</tr>
<tr>
<td><strong>Password Complexity</strong></td>
<td></td>
</tr>
<tr>
<td>Allow user name or its reverse form</td>
<td>Turns off the protection against a password containing the user’s login name or its reverse.</td>
</tr>
<tr>
<td>Lowercase letters</td>
<td>The number of lowercase letters (a-z) that a password must contain.</td>
</tr>
<tr>
<td>Uppercase letters</td>
<td>The number of uppercase letters (A-Z) that a password must contain.</td>
</tr>
<tr>
<td>Numbers</td>
<td>The number of digit characters (0-9) that a password must contain.</td>
</tr>
<tr>
<td>Special characters</td>
<td>The number of non-alphanumeric keyboard characters that a password must contain.</td>
</tr>
<tr>
<td>Maximum consecutive repeated characters</td>
<td>The maximum number of consecutive repeated characters may be the same.</td>
</tr>
</tbody>
</table>

3 Click **Update** to save your settings.

### Configure Session Settings

The RealPresence DMA system enables you to specify the number of simultaneous login sessions by all users and per user ID. You can also configure the length of login sessions.
Note that in a supercluster, the number of used login sessions is the sum of used sessions for all systems that are part of the supercluster.

Similarly, when High Availability is configured, the number of used login sessions is the sum of all used sessions on both systems in the HA pair.

If you plan on having superclustered systems or High Availability paired systems, you need to ensure that you have an adequate number of user login sessions to accommodate simultaneous logins on multiple systems.

**To configure session settings**

1. Go to User > Login Policy Settings > Session.
2. Complete the fields in the following table as needed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active system sessions</td>
<td>Specify the number of simultaneous login sessions by all users or select Unlimited. Note: If this limit is reached, but none of the logged-in users is an Administrator, the first Administrator user to log in is granted access, and the system terminates the non-Administrator session that has been idle the longest.</td>
</tr>
<tr>
<td>Active sessions per user</td>
<td>Specify the number of simultaneous login sessions per user ID or select Unlimited.</td>
</tr>
<tr>
<td>Session hard timeout</td>
<td>Specify the length of time after which the system terminates a session for inactivity.</td>
</tr>
</tbody>
</table>

3. Click Update to save your settings.

**Configure Banner Settings**

A login banner is a message that appears when users attempt to access the system. They must acknowledge the message before they can log in.

From the Banner page, you can enable the banner and select or create the message it displays. The message may contain up to 1500 characters.

**To configure banner settings**

1. Go to User > Login Policy Settings > Banner.
2 Complete the fields in the following table as needed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable login banner</td>
<td>Enables the display of a login banner. If this box is unchecked, the Message field is disabled. The existing contents, if any, remain unchanged, but aren’t displayed to users.</td>
</tr>
<tr>
<td>Message</td>
<td>Select one of the messages from the list, or select Custom and type or paste your own message into the field below. If you select one of the built-in samples, it is copied into the Message field, and you can then edit the copy. When you do so, the system resets the list to Custom. Your edits don’t affect the stored sample. You can revert to the original version of the sample by re-selecting it from the list.</td>
</tr>
</tbody>
</table>

3 Click Update to save your settings.

**Management Access Settings**

The Management Access Settings enable you to restrict access to the management user interface, APIs (port 8443), and SNMP (by default, port 161) to a whitelist of authorized IP addresses or address ranges. If enabled, the whitelist restrictions take effect as soon as you update the settings. If you enable the whitelist and click Update while logged in from an IP address that is not included in the whitelist, the system warns you that you will not be able to access the system and asks you to confirm the update.

The whitelist settings apply to all clusters in a supercluster. When you join a cluster to a supercluster, the cluster’s settings are replaced by those from the supercluster.

**Configure Management Access Settings**

You can add IP addresses and IP address ranges to an authorized whitelist and delete entries from the whitelist when necessary.

To configure management access settings

1 Go to User > Login Policy Settings > Management Access Settings.
2 Add or Delete an IP address or IP address range as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable management access settings&lt;br&gt;Accept management connections from these IP addresses and address ranges on ports 8443 (management user interface/API) and 161 (SNMP)</td>
<td>Enables the input field for IP addresses and restricts management access to the IP addresses or address ranges added to the list. If this box is unchecked, the list and input field are disabled. The existing contents of the list, if any, remain unchanged so that it can be re-enabled at any time without having to re-enter the addresses. <strong>Note:</strong> The label changes to reflect the currently configured SNMP port (see Configure SNMP Settings). Port 161 is the default.</td>
</tr>
<tr>
<td>(list)</td>
<td>Lists the IP addresses and address ranges authorized for management access. Select an entry and click Delete to remove it from the list.</td>
</tr>
<tr>
<td>(input field)</td>
<td>Enter an IP address or address range and click Add to add it to the list. Enter a range as starting and ending IP addresses, separated by a dash. For example: &lt;br&gt;(IPv4) 10.33.33.0 - 10.33.34.255 &lt;br&gt;(IPv6) ::1:ffe - ::2:1</td>
</tr>
</tbody>
</table>

3 Click **Update** to save your settings.
Maintenance

This section provides an introduction to Polycom® RealPresence® DMA® system maintenance. It includes:

- System Management and Maintenance
- System Log Files
- Backing Up and Restoring
- Upgrading the Software
- Shutting Down and Restarting
System Management and Maintenance

The Polycom RealPresence DMA system requires relatively little ongoing maintenance beyond monitoring the status of the system and downloading backups and other data you want to archive. All system management and maintenance tasks can be performed in the management interface. See the appropriate topic for your user role:

- Administrator Responsibilities
- Auditor Responsibilities
- Provisioner Responsibilities

Administrator Responsibilities

As a Polycom RealPresence DMA system administrator, you are responsible for the installation and ongoing maintenance of the system. You should be familiar with the following configurations, tasks, and operations:

- Installing licenses when the system is first installed and when additional call capacity is added.
- Monitoring system health and performing the recommended regular maintenance. See Recommended Regular Maintenance.
- Using the system tools provided to aid with system and network diagnostics, monitoring, and troubleshooting. See Troubleshooting Utilities. Should the need arise, Polycom Global Services personnel may ask you to run these tools.
- Upgrading the system when upgrades/patches are made available. See Upgrading the Software.

Administrator Best Practices

The following are some of our recommendations for administrative best practices:

- Perform the recommended regular maintenance.
- Except in emergencies or when instructed to by Polycom Global Services personnel, don’t reconfigure, install an upgrade, or restore a backup when there are active calls and conferences on the system. Many of these operations will require a system restart to complete, which will result in these calls and conferences being dropped. Before performing these operations, busy out all MCUs and wait for all conferencing activity to cease.
- Before you reconfigure, install an upgrade, or restore a backup, manually create a new backup. Then download and archive this backup in the event that something unforeseen occurs and it becomes necessary to restore the system to a known good state.
- For proper name resolution and smooth network operations, configure two or more DNS servers in your network configuration. This allows the Polycom RealPresence DMA system to function properly in the event of a single external DNS failure.
Configure at least one NTP server in your time configuration and preferably three. Proper time management helps ensure that your cluster operates efficiently and helps in diagnosing any issues that may arise in the future. Proper system time is also essential for accurate audit and CDR data.

**Auditor Responsibilities**

As a Polycom RealPresence DMA system auditor, you're responsible for managing the system's logging and history retention. You should be familiar with the following configurations and operations:

- Configuring logging for the system. See Configure Logging Settings. These settings affect the number and the contents of the log archives available for download from the system. See System Log Files. Polycom Global Services personnel may ask you to adjust the logging configuration and/or download and send them logs.
- Configuring history retention levels for the system. See History Retention Settings. These settings affect how much system activity history is retained on the system and available for download as CDRs. See Call History, Conference History, and Call Detail Records.

**Auditor Best Practices**

The following are some of our recommendations for auditing best practices:

- Unless otherwise instructed by Polycom Global Services, configure logging at the debug level with a rolling frequency of every day and a retention period of 60 days. If hard drive space becomes an issue, decrease the retention period incrementally until the disk space issue is resolved.
- Download log archives regularly and back them up securely (preferably offsite as well as onsite). Delete downloaded log archives to free up disk space.
- Export CDRs regularly and back them up securely (preferably offsite as well as onsite).

**Provisioner Responsibilities**

As a Polycom RealPresence DMA system provisioner, you have access to many of the same features and functions as the system administrator (see User Roles and Access Privileges). Your responsibilities depend on your organization's policies and the tasks delegated to you by the system administrator. For instance, you may be delegated responsibility for some of the following:

- Managing and monitoring users’ conference rooms. See Users.
- Managing and monitoring registered endpoints. See Endpoints.
- Monitoring active calls. See Active Calls.
- Downloading network usage data at the appropriate intervals. See Check Network Usage Data Export and Export Network Usage Data.
- Downloading detailed call and conference history data at the appropriate intervals. See CDR Export and Call Detail Records.
Recommended Regular Maintenance

Perform the following tasks to keep your Polycom RealPresence DMA system operating trouble-free and at peak efficiency. These tasks can be done quickly and should be run at least weekly.

**Archive Backups**

You should archive your backups regularly.

To archive backups:

1. Log into the Polycom RealPresence DMA system
2. Go to Admin > Backup and Restore and check for new backups
   
   If there are new backups, download and archive the latest one. Delete backups after downloading in order to free up disk space.

Every night, each Polycom RealPresence DMA system cluster determines whether its configuration or local user data have changed. If so, it creates a configuration-only backup of the system. For details on backups, see Backing Up and Restoring.

**Check General System Health and Capacity**

You should check your system’s general health and capacity regularly.

To check your system’s general health and capacity:

1. On the Dashboard, verify that:
   a. There are no alerts indicating problems with any part of the system.
   b. The Supercluster Status pane shows the correct number of servers and clusters, and the network interfaces that should be working (depending on your IP type and split network settings) are up (green up arrow) and in full duplex mode, with the speed correct for your enterprise network.
   c. The Cluster Info pane’s Resources section shows that there is adequate free disk space. If the system is using more than 80% of disk space, free up space by doing some or all of the following:
2. Go to Admin > Backup and Restore and download and delete backup files.
3. Go to Admin > System Log Files and download and delete log file archives (you must have the Auditor role to do so.
4. Go to Admin > Server > Logging Settings and reducing the retention period for log archives.
5. Go to Admin > Server > History Retention Settings and reduce the retention values (you must have the Auditor role to do so.
   
   The Territories Status pane shows that all territories have the correct capabilities, are being managed by their primary cluster, and (if your deployment is so configured), have a backup cluster.
6. Go to Monitoring > Network Usage and view the graph for each cluster with the following capacity-related metrics selected:
   
   a. **Call Counts** – If the number of concurrent calls approaches the license limit, you may need to rebalance territory responsibilities, add licensed capacity, or add another cluster.
Conference Manager Calls – If the number of concurrent calls approaches the number of MCU ports available, you may need to add MCU capacity.

- View the graph for each site, site link, and subnet with Calls Dropped and Calls Downspeeded selected. These metrics show only calls dropped or downspeeded due to insufficient bandwidth at the selected throttlepoint. Any values above zero are indicators of bandwidth saturation and suggest that it’s time to increase network bandwidth.

Check Microsoft Active Directory Health

If your RealPresence DMA system is integrated with a Microsoft Active Directory, you can check the health of the Active Directory system.

To check your Microsoft Active Directory health:

1. Go to Reports > MS Active Directory Reports.
2. Check the status and results of the last cache update, and verify that membership information for imported groups, if any, was successfully loaded.
3. Go to Reports > MS Active Directory Reports > Orphaned Groups and Users and verify that the number of orphans is not unexpectedly large.

Check Security Configuration

You should regularly check your RealPresence DMA system's security configuration.

To check your system's security configuration:

- Go to Admin > Server > Security Settings and verify that the security settings are what you expect. Any departure from the settings you expect to see may indicate that your system has been compromised.

Check Certificates

You should regularly check the certificates installed on your RealPresence DMA system.

To check your system's certificates:

1. Go to Admin > Server > Certificates and verify that the list of certificates contains the certificates you have installed (an archived screen capture may be helpful for comparison).
2. Display the details for each certificate you have installed and verify they are accurate (again, an archived screen capture may be helpful for comparison).

Check Network Usage Data Export

You can check your network usage data export. The RealPresence DMA system stores up to approximately 1 GB of network usage data, deleting the oldest as needed. Data size is based on site topology complexity, not usage. On a system with the largest supported site topology, it’s only one day’s worth of usage data, but most systems should retain data for a substantially longer period.
To check your network usage data export:

» Determine an appropriate download interval for your site topology and download network usage data to your local computer during that interval.

**CDR Export**

If you want to preserve detailed call and conference history data in spreadsheet form off the Polycom RealPresence DMA system, periodically download the system’s CDR (call detail record) data to your PC. See *Call Detail Records.*
System Log Files

The System Log Files page lists the available system log file archives and lets you run the following Action list commands:

- **Roll Logs** — Closes and archives the current log files and starts new log files. If you have a supercluster, you’re prompted to choose the cluster whose log files you want to roll.

- **Download Active Logs** — Creates and downloads an archive that contains snapshots of the current log files, but doesn’t close the current log files. If your system is a two-server cluster, in the File Download dialog you can select which server’s logs to download.

- **Download Individual Logs** — Downloads the selected individual log file.

- **Download Archived Logs** — Downloads the selected log file archive.

- **Delete Archived Logs** — Deletes the selected log file archive. Only users with the Auditor role can delete archives, and only archives that have been downloaded can be deleted. We recommend regularly deleting downloaded log file archives in order to free up disk space. (The space allocated for log files depends on the size of the system’s local disk.)

- **Show Download History** — Displays the Download History list for the selected log file archive, showing who downloaded the archive and when. This command is only available if the selected archive has been downloaded.

You can change the logging level, rolling frequency, and retention period in Logging Settings. See Configure Logging Settings.

The archives are Gzip-compressed tar files. Each archive contains a number of individual log files.

The detailed technical data in the log files is not useful to you, but can help Polycom Global Services resolve problems and provide technical support for your system.

In such a situation, your support representative may ask you to download log archives and send them to Polycom Global Services. You may be asked to manually roll logs in order to begin gathering data anew. After a certain amount of the activity of interest, you may be asked to download the active logs and send them to Polycom Global Services.

The following table describes the fields in the System Log Files list.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Date and time that the log file archive was created.</td>
</tr>
<tr>
<td>Host</td>
<td>Host name of the server. When the logs are rolled in a two-server cluster (either automatically or manually), an archive is created for each server.</td>
</tr>
<tr>
<td>Filename</td>
<td>Name of the log file archive.</td>
</tr>
</tbody>
</table>
Working With System Logs

You can manually roll logs, download active, individual, and archived logs, and delete archived logs as needed.

**Manually Roll the System Logs**

Closes and archives the current log files and starts new log files. If you have a supercluster, you’re prompted to choose the cluster whose log files you want to roll.

Manually rolling the system logs instructs the system to close the log files it is currently writing to and begin writing to new log files.

**To manually roll the system logs:**

1. Go to Admin > System Log Files.
2. Under Actions, click Roll Logs.
   
   If you have a supercluster, you’re prompted to choose the cluster whose log files you want to roll.
3. If applicable, select a cluster. Wait a few seconds.
   
   The system closes and archives the current log files and starts writing new ones. A dialog informs you that logs have been rolled, and the new log archive appears in the System Log Files list. For a two-server cluster, an archive is created for each server.
4. Click OK.

**Download Active Logs**

When you download an active log, the RealPresence DMA system creates and downloads an archive that contains snapshots of the current log files, but doesn’t close the current log files. If you have a two-system cluster, you can select which system’s logs to download.

**To download active logs:**

1. Under Actions, click Download Active Logs.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size</td>
<td>Size of the file in megabytes.</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates whether this is an automatic archive, manual archive, or system snapshot archive (created when you download the active logs).</td>
</tr>
</tbody>
</table>

The following table describes the fields in the Download History list.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>The user ID of the person who downloaded the archive.</td>
</tr>
<tr>
<td>Time</td>
<td>Date and time that the archive was downloaded.</td>
</tr>
</tbody>
</table>
2 If you have a two-server cluster, in the Server Name field, select the server with the logs you want to download.

3 Click Download.

4 Depending on your browser, specify a location and file name and then save the file, or check your Downloads folder.

**Download an Individual Log File**

You can select and then download individual active log files.

To download an individual log file:

1 Under Actions, click Download Individual Logs.
   The Download Individual Logs window displays.
2 Select a log file to download and click Download.
3 Depending on your browser, specify a location and file name and then save the file, or check your Downloads folder.

**Download Archived Logs**

If you need to examine log files or send them to Polycom support, you can download log archives to your PC.

To download an archived log:

1 Go to Admin > System Log Files.
2 Select the file you want to download from the list of log archives.
3 Under Actions, click Download Archived Logs.
4 Depending on your browser, specify a location and file name and then save the file, or check your Downloads folder.

**Delete a System Log Archive**

You can delete system log archives to free disk space. Note that only users with the Auditor role can delete archives, and only archives that have been downloaded can be deleted.

To delete a system log archive:

1 Go to Admin > System Log Files.
2 View the Latest Download column to determine if the log archive you want to delete has been downloaded at least once and can be deleted.
3 Select the log archive to delete and verify that the Show Download History command displays under Actions.
4 Click Show Download History (optional) to display the Download History list under the list of log archives.
5 Under Actions, click Delete Archived Logs.
6 Click **Yes** to confirm the deletion.
Backing Up and Restoring

Polycom suggests that you back up your Polycom® RealPresence® DMA® system regularly. You can create a system backup either on the local server or transfer backup files to a remote server. Local backups are performed and stored independently of remote backups.

In addition to the backups that you create, each RealPresence DMA system cluster automatically creates a locally-stored configuration-only backup each night. These configuration-only backups include:

- Local user account information (including local data for enterprise users, such as conference room attributes)
- System configuration data
- Supercluster and resource management system integration data (if applicable)

The backup file is for the cluster, but on a two-server cluster, a copy of the backup exists on each server. This ensures that the backup files are available even if one of the servers is not running.

If you want to create a backup that also includes all the transactional data, including logs, CDRs, network usage, and audit (history) data, you should create these manually or schedule backups to be sent to a remote server on your network. The cluster keeps the most recent ten backups (deleting the oldest backup file when a new one is created).

If you have a superclustered system, you should create backups from each cluster (each cluster’s backup files include only the call, conference, and registration history for that cluster) or transfer the backup files to remote storage.

Download backup files regularly for safekeeping, or transfer them to a remote storage server. The system can locally store up to 10 backup files at one time. Delete backup files after downloading in order to free up disk space on the local system.

In most cases, the software version of the backup file must match the system’s current software version in order to restore from it. But specific releases may include the ability to restore a backup file from specific earlier releases. Check the release notes for your software version for more information.

The option to omit IP network configuration makes it possible to “clone” an existing RealPresence DMA cluster’s feature and system configuration to a new cluster without introducing IP address conflicts.

Backing Up Your System

You can create and download backup files of the RealPresence DMA system, then upload the files and use them to restore the system. You should create and download backups from systems that are part of a supercluster or a High Availability pair.

View Locally Stored Backup Files

You can store up to 10 backup files on the system concurrently and view the stored backup files as needed.
To view locally stored backup files:

» Go to Admin > Backup and Restore.

The following table describes the fields in the Backup and Restore list. The list contains the last 10 backup files.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creation Date</td>
<td>Timestamp of the backup file.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the backup file.</td>
</tr>
<tr>
<td>Size</td>
<td>Size of the backup file.</td>
</tr>
<tr>
<td>System Version</td>
<td>Version number of the application that created the backup file.</td>
</tr>
<tr>
<td>SHA1</td>
<td>SHA1 checksum for the backup file. You can use this to confirm that a</td>
</tr>
<tr>
<td></td>
<td>downloaded file is an exact copy of one on the server.</td>
</tr>
</tbody>
</table>

Create a New Backup File

You can create a configuration-only backup file or a full backup file. A full backup adds all transactional data, including logs, CDRs, network usage, and audit (history) data.

The backup file is for the cluster, but on a two-server cluster, a copy of the backup exists on each server. This ensures that the backup files are available even if one of the servers is not running.

The cluster keeps the most recent 10 backups (deleting the oldest backup file when a new one is created).

To create a new backup file:

1. Go to Admin > Backup and Restore.
2. Verify that the oldest backup file listed is one you do not want to keep or have already downloaded.
3. Under Actions, click Create New (Full) to create a full backup or Create New (Config Only) to create a configuration-only backup (no transaction data).
   
   A confirmation dialog tells you the backup archive was created. For a full backup, this may take some time.
4. Click OK.

Download a Backup File

You can download a backup file to your local computer.

To download a backup file:

1. Go to Admin > Backup and Restore.
   
   The list contains the last ten backup files.
2. Select the backup file you want to download.
3. Under Actions, click Download Selected.
4 Choose a path and filename for the backup file and click **Save**.
   The **File Download** dialog indicates when the download is complete.
5 Click **Close**.

**Upload a Backup File**

You can upload a backup file to the RealPresence DMA system for an immediate restore or in preparation for a future manual system restore from that backup file.

You can store 10 files at a time. Creating a new backup will delete the oldest file (unless there are fewer than 10).

**To upload a backup file:**

1 Go to **Admin > Backup and Restore**.
2 Verify that the oldest backup file listed is one you do not want to keep or have already downloaded.
3 Under **Actions**, click **Upload**.
4 Choose a backup file to upload and click **Open**.
   The system indicates when the upload is complete.
5 Click **Close**.
   The system asks if you want to restore now from the backup file you just uploaded.
6 If you do not want to restore (and restart the system) now, click **Manually Later**.
7 To restore now, click **Now**.
   The **Confirm Restore** dialog appears.
8 Read the confirmation warning, select which data you want to restore, and click **OK**.

Restoring feature and system configuration, but not network configuration (or vice versa) will result in invalid primary or backup cluster assignments for some territories. After the restore operation is complete, go to **Service Config > Site Topology > Territories** and assign primary and backup clusters to the affected territories.

After a short delay, a dialog informs you that the system will be restored and you will be logged out.

9 Click **OK**.
   The system logs you out and the server reboots (typically, this takes about five minutes). After it comes back up, in a two-server cluster, the second server syncs to it, thus being restored to the same state. Depending on the configuration changes being applied, it may reboot so the changes can take effect.
   When done, the LCDs of both the servers display **DMA Clustered** (Polycom Rack Server 630 (R630) or 620 (R620)-based systems only).

10 Log back in as a local **admin** user and:
   a In a two-server cluster, verify on the **Dashboard** that both servers are up and the private network connection is operating properly.
   b Go to **Admin > Software Upgrade** and check the **Operation History** table.
If the system was integrated with Active Directory, go to Integrations > Microsoft Active Directory and re-enable the integration.

**Configure Remote Backup Settings**

You can ease administration of system backups for the cluster by scheduling them to run at certain times and use remote file storage. You can configure the date, start time, and frequency of remote backups, as well as remote storage server details. Scheduling remote backups allows you to more easily archive and retain system backups for use in disaster recovery, if needed.

Remote backups are not stored locally; if the system is unable to store the backup archive on the remote storage server, the scheduled backup fails.

**To configure remote backup settings:**

1. Go to the Admin > Server > Backup Settings page.
2. Select Enable automatic backups of this cluster to a remote server (Remote backups will not be retained locally).
3. Complete the required fields described in the following table:

<table>
<thead>
<tr>
<th>Schedule</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote backup status</td>
<td>Indicates if the system has ever been backed up.</td>
</tr>
<tr>
<td>Last successful remote backup</td>
<td>The read-only date and time of the last successful scheduled backup.</td>
</tr>
<tr>
<td>Next remote backup date</td>
<td>A calendar picker allows you to select the date for the next remote backup.</td>
</tr>
<tr>
<td>Remote backup start time</td>
<td>The time of day that the backup should begin. <strong>Note:</strong> As a best practice, schedule system backups during hours of light system load. This will avoid possible backup-related performance issues during peak hours.</td>
</tr>
<tr>
<td>Frequency of remote backups (In days)</td>
<td>The number of days between backups at this scheduled time. If you choose 1, the scheduled backup will occur every day. The default value is 7.</td>
</tr>
</tbody>
</table>
| Backup type | The type of backup the system should perform:  
  • Config only - A backup containing system settings only (no transaction data).  
  • Full - A complete system backup (configuration and transaction data). The default is Full. |
### Remote server

<table>
<thead>
<tr>
<th>Transfer protocol</th>
<th>Choose one of the following protocol t when transferring files to the remote storage server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP</td>
<td></td>
</tr>
<tr>
<td>HTTP</td>
<td></td>
</tr>
<tr>
<td>HTTPS</td>
<td></td>
</tr>
<tr>
<td>SFTP</td>
<td>The default is SFTP.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hostname or IP address of remote server</th>
<th>The hostname or IP address of the remote storage server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote port</td>
<td>The port the system should use when connecting to the remote server.</td>
</tr>
<tr>
<td>Username</td>
<td>The username the system should use when logging in to the remote storage server.</td>
</tr>
<tr>
<td>Password</td>
<td>The password the system should use when logging in to the remote storage server.</td>
</tr>
<tr>
<td>Remote directory</td>
<td>The directory in which the system should store the backup archive on the remote storage server.</td>
</tr>
<tr>
<td></td>
<td>The directory path must be less than 1000 characters in length and use the forward slash directory delimiter.</td>
</tr>
</tbody>
</table>

4 Test the settings by clicking **Test Settings**.

The system creates an empty archive and attempts to transfer it to the remote backup server using the configured settings. If successful, a dialog appears confirming the success. If the test fails, a dialog appears stating the reason for the failure.

5 Click **Update** to save the settings on this page.

You can initiate a remote backup immediately by clicking the **Backup Now** button.

### Restoring Your System

You can restore system data from a backup file that is stored on the cluster or from a backup file stored on a USB flash drive. Restore from a backup only when there is no activity on the system. Restoring terminates all conferences and reboots the system.

You cannot restore a cluster while it is part of a supercluster. You must manually leave the supercluster first. If the cluster is responsible for any territories (as primary or backup), you must re-assign those territories after restoring the system.

For a two-server cluster, you need to restore the system only when both servers are running and clustered.

Note that if you are restoring a backup and the system was integrated with a Polycom RealPresence Resource Manager system when the backup you are restoring was made, that integration is restored. If the system was not integrated when the backup was made, it will no longer be integrated after restoring.

Both types of restore require you to re-integrate with Active Directory after the restore is complete.
Restoring from a Backup File on the Cluster

You can restore system data from a backup file that is stored on the cluster. Before doing so, ensure that there are no running conferences on the system. You should also make sure that all MCUs are out of service. When restoring a two-server cluster, make sure that both servers are running and clustered. Make sure that there are no calls on the system, and that all MCUs are out of service.

If you are restoring a cluster that is part of a supercluster, you must first remove the cluster from the supercluster.

If you have integrated your system with Active Directory, you will need to re-do the integration after restoring from a backup file.

To restore from a backup file on the cluster:

1. Go to Admin > Backup and Restore.
2. Select the backup file from which you want to restore.
3. Under Actions, click Restore Selected.
   - If the backup file you selected is from a different version of the software, the system displays a warning of the possible consequences if you restore.
4. Confirm that you want to continue.
5. Select the data you want to restore. The data you can restore depends on:
   - The type of backup file (full or config-only) you selected.
   - For a restore from a non-identical software version, which restore operations the current version supports for the source version data.
   - The options may include:
     - IP network configuration
     - Feature and system configuration
     - History, network usage, and log data
   - Restoring feature and system configuration but not network configuration (or vice versa) will result in invalid primary or backup cluster assignments for some territories. After the restore operation is complete, go to Service Config > Site Topology > Territories and assign primary and backup clusters to the affected territories.
6. Click OK.
7. After a short delay, a message informs you that the system will be restored and you will be logged out.
8. Click OK.
   - The system logs you out and reboots (typically, this takes about five minutes). After the system restarts, in a two-server cluster, the second server syncs to it, restoring it to the same state. Depending on the changes being applied, it may reboot so the changes can take effect.
   - When done, the LCDs of both display DMA Clustered. (Polycom Rack Server 630 (R630) or 620 (R620)-based systems only).
9. Log back in as a local admin user and verify the restore:
a In a two-server cluster, verify on the Dashboard that both servers are up and the private network connection is operating properly.

b Go to Admin > Software Upgrade and check the Operation History table.

c If the system was integrated with Active Directory, go to Integrations > Microsoft Active Directory and re-enable the integration.

**Restore from a Backup File on the Polycom RealPresence DMA System’s USB Flash Drive**

If the system is shut down or in a bad state, you can use the Polycom RealPresence DMA USB Configuration Utility to restore the RealPresence DMA system from a backup file (full or configuration-only) that you load onto the USB flash drive.

Note that when you use the USB Configuration Utility to restore a backup, you cannot select which data to restore. If you copy a config-only backup file to the USB flash drive, both the feature and system configuration data and the IP network configuration data will be restored. If you copy a full backup file to the USB flash drive, the transactional (historical) data will also be restored.

If you restore a cluster using the USB Configuration Utility while it is part of a supercluster, it’s automatically removed from the supercluster.

When you restore from a backup file stored on a flash drive, you must first shut down the system.

Only backups from identical versions of the software can be restored using the USB Configuration Utility.

**To restore from a backup file on the Polycom RealPresence DMA system’s USB flash drive:**

1. If the system is running and accessible, log in as an Administrator, make sure that there are no calls on the system and that all MCUs are out of service.

2. Shut down the system.

3. Connect the USB memory stick containing the RealPresence DMA USB Configuration Utility (included with your Polycom RealPresence DMA system) to a Windows PC.


   If autorun does not work or is turned off, navigate to the USB memory stick using My Computer, Windows Explorer, or another file manager. Then start the Configuration Utility by double-clicking_dma7000-usb-config.exe.
5 In the DMA USB Configuration Utility window, click Copy a Backup to the USB flash drive.

6 Select the backup file from which you want to restore the system and click Open.

   The utility displays an error message if the file isn't a valid Polycom RealPresence DMA system backup. Otherwise, it confirms that the backup file is in place.

   The utility's main window states that The USB flash drive is ready to restore the system from a backup file. At the bottom of the window, it displays information about the selected backup file.

7 Close the utility.

8 In your system tray, click Safely Remove Hardware and select Safely Remove USB Mass Storage Device. When a message tells you it is safe to do so, disconnect the USB memory stick from the PC and take it to the data center housing the Polycom RealPresence DMA system server(s).

9 Make sure that the server or servers are turned off. Then insert the USB flash drive into a USB port on one of the servers and turn that server on (but not the other, if there are two).

   If this cluster is part of a supercluster, it is automatically removed from the supercluster. The server boots and the data in the backup file is applied. Typically, this takes about five minutes. Depending on the configuration changes being applied, the server may reboot so the changes can take effect.

10 If this is a two-server cluster:

   a For a Polycom Rack Server 630 (R630) or 620 (R620)-based cluster: After the first server has rebooted (if necessary) and its front-panel LCD displays DMA Ready, turn on the second server.

      The second server boots, finds the first server, and syncs to it, thus being restored to the same state. Depending on the configuration changes being applied, it may reboot so the changes can take effect.

      When done, the LCDs for both the servers display DMA Clustered.
For a Polycom Rack Server 220-based cluster: After the first server has rebooted (if necessary) and has been running for at least 10 minutes, turn on the second server.

The second server boots, finds the first server, and syncs to it, thus being restored to the same state. Depending on the configuration changes being applied, it may reboot so the changes can take effect.

11 Log back in as a local admin user and verify the restore:

a In a two-server cluster, verify on the Dashboard that both servers are up and the private network connection is operating properly.

b Go to Admin > Software Upgrade and check the Operation History table.

c If the system was integrated with Active Directory, go to Integrations > Microsoft Active Directory and re-enable the integration.
Upgrading the Software

You can upload a RealPresence DMA software upgrade package and install the upgrade on your system. You can also roll back to the previous version, if necessary.

The upgrade process can be used for patches, minor upgrades, and major upgrades. In all three cases, the current system configuration (including users, MCUs, Conference Manager settings, and Call Server settings) is preserved.

Patches do not require new license keys, but major and minor version upgrades do. Any of the three upgrades may require a system restart.

Upgrading Overview

Always check the upgrade version release notes before installing an upgrade.

The Basic Upgrade Procedure is for:

- Installing any software upgrade on a single-server or two-server system that’s not part of a supercluster.
- Installing a patch (supercluster-compatible software upgrade) on a cluster that’s part of a supercluster. In that case, you repeat the procedure on each cluster.

To apply a major or minor software upgrade to a superclustered system, see Perform a Minor or Major Upgrade on a Superclustered System.

The upgrade installation process automatically creates a backup, which enables you to roll back an upgrade (restore the previous version) if necessary. As a precaution, however, you should download a recent backup file or take a snapshot of your Virtual Edition instance before you begin to install an upgrade. See Backing Up and Restoring.

You can roll back only the last applied upgrade. Rolling back an upgrade restores the database to its state prior to the upgrade, so data may be lost.

During an upgrade or rollback procedure, you may need to refresh (or restart) your browser or clear your browser’s cache before you log back in to the RealPresence DMA management user interface. This helps to ensure that all system information you view is accurate and current.

Upgrading Preparation

Consider the following points to prepare for upgrading:

- If the upgrade requires a new license, obtain the license activation keys or licensing server IP address before you upgrade.

- If upgrading an Appliance Edition System, download a recent backup and upload the upgrade package file before you plan to upgrade. For a supercluster, do this on each cluster.
Perform the remainder of the procedure during a maintenance window then there are no calls or conferences so that you can immediately take the cluster out of service instead of having to wait for all call activity to end. This also eliminates concerns about whether the remaining clusters of a supercluster have sufficient capacity to handle the load of the cluster being upgraded.

**View Software Upgrade Information**

The software upgrade page lists current version information, any upgrade packages you have uploaded, and upgrade operation history.

**To view software upgrade details**

1. Go to **Admin > Software Upgrade**.
2. Review the software upgrade details as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version Information</td>
<td>Shows the current system version and the rollback version (if any), which is the previous system version.</td>
</tr>
<tr>
<td>Upgrade Package Details</td>
<td>Shows the version number and other information about the upgrade file that’s been uploaded (if any). Also indicates whether the system must be restarted after upgrading and displays a brief description, which includes an estimated install time.</td>
</tr>
<tr>
<td>Operation History</td>
<td>Lists each upgrade management operation (upgrade or downgrade), showing the server on which it was performed, package version, date of the operation, and which user performed it.</td>
</tr>
</tbody>
</table>

**Upload the Upgrade Package**

Before upgrading, you need to save the upgrade package file at a location on or accessible from your PC.

**To upload an upgrade package:**

1. Go to **Admin > Software Upgrade**.
2. In the **Actions** list, click **Upload**.
3. Select the upgrade package file and click **Open**. The **File Upload** window indicates when the upload is complete.
4. Click **Close**. The **Upgrade Package Details** section displays information about the file you uploaded. The description includes an estimated install time.
5. Verify that the upgrade package is correct.

**Prepare Your Supercluster**

If the cluster you are upgrading is part of a supercluster, you need to remove the cluster from the supercluster before upgrading it. Each cluster must be upgraded individually.
To prepare your supercluster for upgrade:

1. Log in to the RealPresence DMA system you are upgrading and go to Service Config > Site Topology > Territories.
2. Reassign the system’s territory responsibilities.
3. Log in to a different RealPresence DMA system and verify that the territory change has been replicated.
4. Go to Integrations > DMA and stop using the system you are upgrading, or busy it out and wait for all calls to end.
5. Click Remove from Supercluster, then click Yes to confirm.
   The cluster is removed from the supercluster. The system informs you when the process is complete, then logs you out and restarts.
6. Click OK to log out immediately or wait for the system to log you out.
7. Wait for approximately five minutes before trying to log back in to the system.
   You may need to restart your browser or clear your browser cache to log back in.
8. Log back in to the system you removed and verify on the Supercluster Status pane of the Dashboard that the system is no longer part of the supercluster.

Basic Upgrade Procedure

Use the Basic Upgrade Procedure to do the following:

- Install any software upgrade on a single-server or two-server system that is not part of a supercluster.
- Install a patch (supercluster-compatible software upgrade) on a cluster that is part of a supercluster.
  In this case, you repeat the procedure on each cluster.

To apply a minor or major software upgrade to a superclustered system, see Perform a Minor or Major Upgrade on a Superclustered System.

Upgrade the Software

After you have uploaded the upgrade package to a local PC, you can upgrade the software. Ensure that there are no running conferences on the system before proceeding.

To upload and install an upgrade file:

1. Go to Admin > Software Upgrade.
2. Click Upload.
3. Select the upgrade package file and click Open.
   The system indicates when the upload is complete.
4. Click Close.
   The Upgrade Package Details section displays information about the file you uploaded and an estimated install time.
5. Verify that the upgrade package is correct.
   If a system restart is required, make sure no calls are in progress on the system.
6 If this system is part of a supercluster, do the following:
   a Go to Service Config > Site Topology > Territories and reassign the system’s territory responsibilities. Wait a few minutes and verify on another cluster that the change has been replicated.
   b Go to Integrations > DMA and stop using the system you are upgrading, or busy it out and wait for all calls to end.
   c Click Remove from Supercluster, then click Yes to confirm.
      The cluster is removed from the supercluster. The system informs you when the process is complete, then logs you out and restarts.
   d Click OK to log out immediately or wait for the system to log you out.
      Wait for approximately five minutes before trying to log back in to the system. You may need to restart your browser or clear your browser cache to log back in.
   e Log back in to the system you removed and verify on the Supercluster Status pane of the Dashboard that the system is no longer part of the supercluster.

7 Go to Admin > Software Upgrade.

8 Click Upgrade.

9 Click Yes to confirm you want to upgrade.
   If a restart is required, the system informs you that the upgrade is starting, then logs you out and restarts.

10 Click OK to log out immediately or wait for the system to log you out.
   The Upgrade Status page displays and shows progress and the upgrade logging.

11 When the upgrade and reboot are finished and all necessary system services have started, log back in to the system.
   You may need to restart your browser or clear your browser cache before logging back in.

12 In a two-system cluster, verify on the Dashboard that both systems are up and the private network connection is operating properly.

13 Go to Admin > Software Upgrade and view the Operation History table to ensure the upgrade was successful.

14 If the upgrade requires a new license or licenses, obtain and install them as described in Adding Licenses.

Perform a Minor or Major Upgrade on a Superclustered System

All clusters within a supercluster must be upgraded individually. During this process, software versions between clusters will not be compatible until all clusters have been upgraded to the new version.

You have two options for upgrading a supercluster:
   ● Perform the cluster upgrades in a system-wide maintenance window during which all the clusters can be shut down and the service is completely unavailable. This is the simplest and fastest method.
Perform the cluster upgrades incrementally so that some system capacity (although reduced) remains available during the process. This method is more complex, error-prone, and lengthy.

During the course of an incremental upgrade, some clusters will be running the new software version while others will still be running the older version, effectively creating two separate superclusters until all the clusters are upgraded. Configuration changes are necessary for some level of service to remain available, and the configuration changes must be repeated as each cluster is removed from the original supercluster, upgraded, and added to the new supercluster.

Before deciding to perform an incremental upgrade, carefully read and consider the information in Factors to Consider for an Incremental Supercluster Upgrade.

**Upgrade a Supercluster During a Complete Service Outage**

You can upgrade a supercluster during a complete service outage. If it is possible to schedule the upgrade for a maintenance window during which there is no service, Polycom recommends doing so.

To minimize the time required for an upgrade:

- Obtain the license activation keys ahead of time.
- On each cluster, download a recent backup and upload the upgrade package file (the first two steps below) ahead of time.

**To upgrade a supercluster during a complete service outage:**

1. Save the upgrade package file somewhere on or accessible from your PC.
2. On each cluster in the supercluster, do the following:
   a. Go to **Admin > Software Upgrade**.
   b. In the **Actions** list, click **Upload**.
   c. Select the upgrade package file and click **Open**.
      - The **File Upload** dialog indicates when the upload is complete.
   d. Click **Close**.
      - The **Upgrade Package Details** section displays information about the file you uploaded. The description includes an estimated install time.
   e. Verify that the upgrade package is correct.
3. On any cluster in the supercluster, do the following:
   a. Go to **Service Config > Site Topology > Territories** and record each territory’s primary and backup cluster and whether it hosts conference rooms and associated sites.
      - You may need this information later to restore the configuration.
   b. If there are no active calls and conferences, click **Close**. Otherwise, go to **Integrations > DMA** and busy out each cluster in the supercluster.
      - This permits existing calls and conferences to continue, but prevents new conferences and point-to-point calls from starting.
   c. On the Dashboard, monitor the **Call Server Active Calls** and **Conference Manager MCUs** panes.
   d. When all calls and conferences have ended, go to **Integrations > DMA** and stop using each cluster in the supercluster.
      - This completely shuts down the supercluster.
4 On the cluster you are logged in to (e.g., cluster A), do the following:
   a Go to Admin > Software Upgrade.
   b In the Actions list, click Upgrade.
   c Click Yes to confirm.
      If a restart is required, the system informs you that the upgrade is starting. Shortly after that, the
      system logs you out and restarts.
   d Click OK to log out immediately, or wait until the system logs you out.
      The Upgrade Status page displays progress and the upgrade logging. When the upgrade is
      complete, the system reboots.

   You can perform steps 5 and 6 to upgrade all the other clusters simultaneously, while the upgrade
   package is being installed on cluster A. If not, you can start upgrading cluster B at this point, and when
   it restarts, start upgrading the next cluster, and so on. You do not need to wait for each cluster
   upgrade to be finished before starting the next one.

When the upgrade and reboot are finished and all necessary system services have started, you are
able to log back in. You may need to restart your browser or clear your browser cache before you can
log back in.

   e Log back in and in a two-server cluster, verify on the Dashboard that both servers are up and the
      private network connection is operating properly.
   f Go to Admin > Software Upgrade and check the Operation History table.
   g If the upgrade requires a new license activation key code or codes, obtain and install them as
      described in Adding Licenses.

5 Log in to one of the other clusters (e.g., cluster B) and do the following:
   a Go to Admin > Software Upgrade.
   b In the Actions list, click Upgrade.
      A confirmation dialog appears.
   c Click Yes.
      If a restart is required, a dialog informs you that the upgrade is starting. Shortly after that, the
      system logs you out and restarts.
   d Click OK to log out immediately, or simply wait.
      When the upgrade process is finished and all necessary system services have finished starting,
      you are able to log back in. You may need to restart your browser or clear your browser cache in
      order to log back into the system.
   e Log back in and, in a two-server cluster, verify on the Dashboard that both servers are up and the
      private network connection is operating properly.
   f Go to Admin > Software Upgrade and check the Operation History table.
   g If the upgrade requires a new license activation key code or codes, obtain and install them as
      described in Adding Licenses.
   h Go to Integrations > DMA and join this cluster to cluster A to create a supercluster.
      You now have a new supercluster consisting of two upgraded clusters.
6 For each additional cluster, repeat step 5 of this procedure to upgrade it and add it to the new supercluster.

7 On any cluster of the new supercluster, do the following:
   a Go to Service Config > Site Topology > Territories and restore the territory assignments. Or, if previously integrated with a Polycom RealPresence Resource Manager system, go to Integrations > RealPresence Resource Manager and reestablish the integration.
      Integration with a RealPresence Resource Manager system imports the site topology data, including territory assignments, from that system.
   b Go to Integrations > DMA and return each cluster to service.
   c Verify, and restore or update if necessary, other supercluster configuration settings.

The supercluster is now fully upgraded.

**Upgrading a Supercluster While Maintaining Partial Service**

Polycom recommends upgrading a supercluster only during a system-wide maintenance window when there are no calls or conferences on the system and all clusters can be taken out of service. This decreases the time required to upgrade the supercluster.

If you upgrade incrementally, be aware of the limited capacity available at any point in the process. There should be little or no conferencing activity in any territory until after the new supercluster has been created and responsibilities for that territory have been reassigned to a cluster in the new supercluster.

To minimize the time required for an upgrade:

- If the upgrade requires a new license, obtain the license keys ahead of time.
- Download a recent backup and upload the upgrade package file to all clusters in the supercluster ahead of time.

**Factors to Consider for an Incremental Supercluster Upgrade**

Before deciding to perform an incremental supercluster software upgrade, be aware of the following:

- An incremental upgrade can take five times as long as the simplified method.
- As clusters are removed from the existing supercluster and upgraded, its capacity is reduced. As the new supercluster is being built, it will not be at full capacity until all clusters are upgraded. Both the existing supercluster and the new one will have limited capacity until completely upgraded, with the following possible consequences:
   - Some endpoints may be unable to register.
   - The MCUs remaining in the supercluster may not have the capacity to handle all the conferences.
   - Some endpoints may not successfully redirect their registrations and may not be able to make or receive calls.
- As the old supercluster is deconstructed, the territory associations have to be changed each time a cluster leaves. As the new supercluster is built, the territory associations have to be changed each time a cluster joins.
- As the clusters for some endpoints are removed from the existing supercluster and join the new one, the video network becomes partitioned with separate islands of endpoints.
• Some endpoints do not respond well to a gatekeeper change (such as a signaled alternate gatekeeper). To successfully redirect these endpoints to a Call Server in the new supercluster, one of the following may be necessary:
  - Managed endpoints may be re-provisioned by the Polycom RealPresence Resource Manager system, or third-party endpoint management system responsible for them.
  - Unmanaged endpoints may be manually reconfigured and restarted if necessary (in some cases, restarting an endpoint may be sufficient).
• Any configuration changes to the old supercluster (once the first cluster has left) may be lost when the new supercluster is created.
• History records for calls and conferences that cross from the old supercluster to the new one (and vice versa) will not be merged into a single call/conference after the upgrade.
• If embedded DNS is enabled, the enterprise DNS can only point to one supercluster. The other supercluster will not have territory fail-over capability.
• If Conference Manager is enabled, during the time that the supercluster is split into two, each supercluster could host separate conferences on the same VMR.

The site topology bandwidth specifications will be duplicated in both the old supercluster and the new supercluster. Without significant changes to the site topology’s bandwidth configuration, this can lead to bandwidth overloading during the upgrade.

Rolling Back System Software to Previous Versions

After you upgrade your system software to a new version, you can roll back the upgrade to restore the previous version of software you were running. However, if a rollback is necessary, you may need to reconfigure supercluster or High Availability (HA) configuration settings for your system(s).

The state of a RealPresence DMA system after you perform an upgrade and then roll back to the previous version may vary, depending on the software version from which you upgraded and whether you configured some of your system settings before performing a rollback.

The following table describes the states of a RealPresence DMA system before and after an upgrade and after a rollback.

<table>
<thead>
<tr>
<th>System Version and State Before Upgrade</th>
<th>System State After Upgrade and Additional Configuration</th>
<th>System Version and State After Rollback</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.0.x – Standalone single-server cluster</td>
<td>Part of an HA pair or supercluster</td>
<td>9.0.x – Standalone single-server cluster</td>
</tr>
<tr>
<td>9.0.x – Part of an HA pair or supercluster</td>
<td>Part of an HA pair or supercluster</td>
<td>9.0.x – Part of an HA pair or supercluster</td>
</tr>
<tr>
<td>6.4.x – Standalone single-server cluster</td>
<td>Part of an HA pair or supercluster</td>
<td>6.4.x – Standalone single-server cluster; cannot pair or supercluster with 9.0.x systems.</td>
</tr>
<tr>
<td>6.4.x – Part of an HA pair or supercluster</td>
<td>Part of an HA pair or supercluster</td>
<td>6.4.x – Standalone single-server cluster; cannot pair or supercluster with 9.0.x systems; may be able to pair or supercluster with 6.4.x systems.</td>
</tr>
</tbody>
</table>
After rolling back superclustered systems to version 6.4.x, the systems may be able to re-establish supercluster communications, but this is not guaranteed.

**Roll Back an Upgrade**

You can roll back an upgrade to restore the previous software version. Note that rolling back a system version terminates active calls and conferences and requires a system restart.

To roll back an upgrade, restoring the previous version:

1. Go to Admin > Software Upgrade.
2. Verify that you want to downgrade the system to the rollback version shown and that you are prepared for a system restart, if required.
   - Most rollbacks will require a restart.
3. If this cluster is part of a supercluster and you are rolling back after rejoining the supercluster, do the following:
   - If integrated with a Polycom RealPresence Resource Manager system, go to Integrations > RealPresence Resource Manager and terminate the integration.
   - Go to Service Config > Site Topology > Territories and reassign the cluster's territory responsibilities. Wait a few minutes and verify on another cluster that the change has been replicated.
   - Go to Integrations > DMA and take this cluster out of service (or busy it out and wait for all calls to end).
   - Select this cluster and click Remove from Supercluster.
   - Click Yes to confirm.
   - The cluster is removed from the supercluster. The system informs you when the process is complete, logs you out, and restarts.
   - Click OK to log out immediately, or simply wait.

   Wait for approximately five minutes before trying to log back into the system. You may need to restart your browser or clear your browser cache in order to log back in.

   - Log back in to the cluster you removed.
   - Wait for approximately five minutes before trying to log back in to the system. You may need to restart your browser or clear your browser cache in order to log back in.
   - Verify on the Supercluster Status pane of the Dashboard that the cluster is no longer part of the supercluster.
   - Return to Admin > Software Upgrade.
4. In the Actions list, click Roll Back.
5. Click Yes to confirm the rollback.
   - If a restart is required, the system informs you that the downgrade is starting. Shortly after that, the system logs you out and restarts.
6 Click **OK** to log out immediately, or simply wait.

When the downgrade process is finished and all necessary system services have started, you are able to log back in. You may need to restart your browser or clear your browser cache to be able to log back into the system.

7 Log back in and do the following:

   a  In a two-system cluster, verify on the **Dashboard** that both systems are up and the private network connection is operating properly.

   b  Go to **Admin > Software Upgrade** and check the **Operation History** table.

8 If this cluster is part of a supercluster, do the following:

   a  Go to **Integrations > DMA**, and rejoin this cluster to the supercluster.

   ![WARNING]

   Be sure you select the cluster you just downgraded (the one you are logged in to) and join it to another cluster, not the other way around.

   b  Go to **Service Config > Site Topology > Territories** and reassign territory responsibilities back to this cluster. Or, if previously integrated with a Polycom RealPresence Resource Manager system, go to **Integrations > RealPresence Resource Manager** and reestablish the integration.

   Integration with a RealPresence Resource Manager system imports the site topology data, including territory assignments, from that system.
Shutting Down and Restarting

The Polycom RealPresence DMA system’s Shutdown and Restart page lets you restart the system or turn it off completely. In a two-server cluster, you can shut down or restart either one or both servers in the cluster. There is no mechanism for shutting down an entire supercluster at once. If you want to shut down all clusters in a supercluster, you must do so one cluster at a time. Wait at least five minutes before shutting down the next cluster.

If you want to shut down a cluster in the supercluster while other clusters remain on, remove the cluster from the supercluster if it will remain shut down for more than a few hours. The supercluster retains only a limited amount of “playback” data that can be used to bring the shutdown cluster back up to date once it’s turned back on. If the cluster remains off long enough, its data store cannot be made consistent with the rest of the supercluster.

Both shutting down and restarting will terminate all existing calls and log out all current users.

Do not turn off a Polycom RealPresence DMA system server by simply unplugging it or otherwise removing power, especially if it’s going to remain off for some time. If a server loses power without being properly shut down, the RAID controller fails to shut down, eventually depleting its battery. If that happens, the server cannot be restarted without user input, requiring a keyboard and monitor.

Restart or Shut Down One or Both Servers in a Cluster

From the Shutdown and Restart page, you can restart or shut down one or both servers in a cluster.

To restart or shut down one or both servers in a cluster

1. Go to Admin > Shutdown and Restart.
   The page displays the server or servers in the cluster, along with status information.
2. Select the server(s) you want to shut down or restart.
3. Do one of the following:
   a. To restart the selected server(s), click Restart.
   b. To shut down the selected server(s), click Shut Down.
4. When asked to confirm that you want to restart or shut down, click Yes.
   The system logs you out and the selected server(s) shut down. If you chose Restart, the servers reboot and the conference service becomes available again when the restart is complete. If you chose Shut Down, the servers remain powered off until you manually turn them back on.

To shut down all clusters in a supercluster, repeat the above procedure on each additional cluster, waiting at least five minutes between clusters.
Start Up a Shut-Down Cluster

Follow this procedure to start up a cluster that has been powered down.

To start up a shut-down cluster

1. Turn on the first server in the cluster.
   The server boots, which takes several minutes.
2. Wait at least one minute and turn on the second server in the cluster.
   The second server boots. When done, the LCDs of both the servers display DMA Clustered (applies to Polycom Rack Server 630 or 620-based systems only).

To start up all clusters in a supercluster, repeat the above procedure on each additional cluster, waiting at least five minutes between clusters. After all clusters have restarted, it may take up to 30 minutes for all supercluster-wide replication to complete.
Monitoring

This section provides an introduction to monitoring the Polycom® RealPresence® DMA® system. It includes:

- Active Calls
- Endpoints
- High Availability Status
- Login Sessions
- Site Statistics
- Site Link Statistics
- SNMP Monitoring
Active Calls

From the **Active Calls** page, you can monitor the calls in progress (managed by the Call Server) and disconnect an active call.

The search pane above the two lists lets you find calls matching the criteria you specify. Click the filter icon to expand the search pane. You can search for an originator or destination device by its name, alias, or IP address. You can limit your search by specifying one or more of the following:

- Cluster, territory, or site.
- Signaling type (H.323 or SIP) or registration status of the call originator.
- Class of service or bit rate range.

The system matches any string you enter against the beginning of the values for which you entered it. If you enter “10.33.17” in the **Originator** field, it displays calls from devices whose IP addresses are in that subnet. To search for a string not at the beginning of the field, you can use an asterisk (*) as a wildcard.

Leave a field empty (or select the blank entry from a list) to match all values.

The calls that match your search criteria (up to 500) appear in the lower list. You can pin a call that you want to review. This moves it to the upper list, and it remains there, even after the call ends, until you unpin it.

Details about the selected call are available in the **Call Info**, **Originator**, **Destination**, and **Bandwidth** tabs of the pane on the right. This information (and more) is also available in the **Call Details** dialog, which appears when you click **Show Call Details** (in the **Actions** list).

**Note:** If a call traverses multiple clusters in a supercluster, it is counted as a single call, but it appears in the results of each cluster it touches when you search by cluster. Therefore, the sum of the number of calls for each cluster may be greater than the total number of calls for the entire supercluster.

### View the Active Calls List

You can view the **Active Calls** list for reference.

#### To view the active calls list:

- Go to **Monitoring > Active Calls**.

  The following table describes the **Active Calls** list.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✴ (Pin State)</td>
<td>Click to pin a call, moving it to the top list and keeping its information available even if the call ends. Click again to unpin it.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Time the call began (first signaling event).</td>
</tr>
</tbody>
</table>
View Call Details

You can view a call’s details, which provide specific information about the selected call. Note that some of the Call Server Settings can affect the values reflected for a call.

A fully-external call is a call that the RealPresence DMA system is aware of and for which it has an audit record. However, a fully-external call’s signaling does not pass through the RealPresence DMA system so these calls do not have signaling diagrams.

To view call details:

1. Go to Monitoring > Active Calls.
2. Select the call of interest and click Show Call Details to display the following call details:

<table>
<thead>
<tr>
<th>Tab/Field/Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Info</td>
<td>Displays the call’s:</td>
</tr>
<tr>
<td></td>
<td>• Status (active/ended and pinned/unpinned)</td>
</tr>
<tr>
<td></td>
<td>• Start time and end time</td>
</tr>
<tr>
<td></td>
<td>• Duration</td>
</tr>
<tr>
<td></td>
<td>• Signaling protocol(s)</td>
</tr>
<tr>
<td></td>
<td>• Polycom RealPresence DMA server(s) involved</td>
</tr>
<tr>
<td></td>
<td>• Unique call ID</td>
</tr>
<tr>
<td></td>
<td>• Dial string, if available</td>
</tr>
<tr>
<td></td>
<td>• Final dial string (after processing by dial rules)</td>
</tr>
</tbody>
</table>
### Originator
Displays the source device’s:
- Name and authentication name
- Authentication status
- Model and version
- Aliases
- IP address or host name
- Registration status
- Site and territory
If this is a registered endpoint or a registered/configured MCU, a link takes you to the corresponding page with that endpoint or MCU selected.

### Destination
Displays the destination device’s:
- Name and authentication name
- Authentication status
- Model and version
- Aliases
- IP address or host name
- Registration status
- Site and territory
If this is a registered endpoint or a registered/configured MCU, a link takes you to the corresponding page with that endpoint or MCU selected.

### Bandwidth
Available only after the call has ended. The table at the top lists each throttle point that the call traverses and shows its:
- Bit rate limit per call (kbps)
- Total capacity (kbps)
- Used bit rate (kbps) in each class of service
- Weight (%)
- Territory
If the throttle point is a subnet, site, or site link, a link takes you to the corresponding site topology page with the throttle point entity selected.
Below the table, the data used in bandwidth processing is displayed (all bit rates are kbps):
- Formal maximum bit rate limit — the maximum allowed bit rate considering the per call bit rates of each throttle point, but not considering total capacity or current usage
- Available bit rate capacity in each class of service and for the call’s class
- Class of service for the call
- Minimum downspeed bit rate
- Available bit rate limit (%) — the maximum percentage of remaining bandwidth at a throttle point that will be given to any one call (configurable in the Call Server Settings)
- Requested bit rate
- Final bit rate

<table>
<thead>
<tr>
<th>Tab/Field/Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Originator</td>
<td>Displays the source device’s:</td>
</tr>
<tr>
<td></td>
<td>- Name and authentication name</td>
</tr>
<tr>
<td></td>
<td>- Authentication status</td>
</tr>
<tr>
<td></td>
<td>- Model and version</td>
</tr>
<tr>
<td></td>
<td>- Aliases</td>
</tr>
<tr>
<td></td>
<td>- IP address or host name</td>
</tr>
<tr>
<td></td>
<td>- Registration status</td>
</tr>
<tr>
<td></td>
<td>- Site and territory</td>
</tr>
<tr>
<td></td>
<td>If this is a registered endpoint or a registered/configured MCU, a link takes you to the corresponding page with that endpoint or MCU selected.</td>
</tr>
<tr>
<td>Destination</td>
<td>Displays the destination device’s:</td>
</tr>
<tr>
<td></td>
<td>- Name and authentication name</td>
</tr>
<tr>
<td></td>
<td>- Authentication status</td>
</tr>
<tr>
<td></td>
<td>- Model and version</td>
</tr>
<tr>
<td></td>
<td>- Aliases</td>
</tr>
<tr>
<td></td>
<td>- IP address or host name</td>
</tr>
<tr>
<td></td>
<td>- Registration status</td>
</tr>
<tr>
<td></td>
<td>- Site and territory</td>
</tr>
<tr>
<td></td>
<td>If this is a registered endpoint or a registered/configured MCU, a link takes you to the corresponding page with that endpoint or MCU selected.</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Available only after the call has ended. The table at the top lists each throttle point that the call traverses and shows its:</td>
</tr>
<tr>
<td></td>
<td>- Bit rate limit per call (kbps)</td>
</tr>
<tr>
<td></td>
<td>- Total capacity (kbps)</td>
</tr>
<tr>
<td></td>
<td>- Used bit rate (kbps) in each class of service</td>
</tr>
<tr>
<td></td>
<td>- Weight (%)</td>
</tr>
<tr>
<td></td>
<td>- Territory</td>
</tr>
<tr>
<td></td>
<td>If the throttle point is a subnet, site, or site link, a link takes you to the corresponding site topology page with the throttle point entity selected.</td>
</tr>
<tr>
<td></td>
<td>Below the table, the data used in bandwidth processing is displayed (all bit rates are kbps):</td>
</tr>
<tr>
<td></td>
<td>- Formal maximum bit rate limit — the maximum allowed bit rate considering the per call bit rates of each throttle point, but not considering total capacity or current usage</td>
</tr>
<tr>
<td></td>
<td>- Available bit rate capacity in each class of service and for the call’s class</td>
</tr>
<tr>
<td></td>
<td>- Class of service for the call</td>
</tr>
<tr>
<td></td>
<td>- Minimum downspeed bit rate</td>
</tr>
<tr>
<td></td>
<td>- Available bit rate limit (%) — the maximum percentage of remaining bandwidth at a throttle point that will be given to any one call (configurable in the Call Server Settings)</td>
</tr>
<tr>
<td></td>
<td>- Requested bit rate</td>
</tr>
<tr>
<td></td>
<td>- Final bit rate</td>
</tr>
</tbody>
</table>
### Tab/Field/Column | Description
---|---
**Call Events** | Lists each call event in the call and its attributes. When the system is operating as a SIP proxy server, the list includes all SIP signaling messages except 100 TRYING. Hover over an attribute label to see a description. Click **Show Message** to see the signaling message. Click **Show QoS Data** to see detailed quality of service statistics.

**Subscription Events** | For conference (VMR) calls, lists SUBSCRIBE/NOTIFY events, if any, associated with this call. The SIP SUBSCRIBE/NOTIFY conference notification service (as described in RFCs 3265 and 4575), allows SIP devices (generally, conference participants) to subscribe to a conference and receive conference rosters and notifications of conference events. The rosters identify the participants, their endpoints, and their video streams. Hover over an attribute label to see a description. Click **Show Message** to see the signaling message. **Note:** If the system is configured to let devices subscribe to a conference without being participants in the conference (see Security Settings), the call history doesn’t include data for such non-participant subscriptions. But be aware that a subscription to a conference by a non-participant consumes a call license.

**Property Changes** | Lists each property change in the call, showing the value, time, and sequence number of the associated event.

**QoS** | Quality of service data is only available if one of the endpoints is a registered H.323 endpoint that supports IRQs. This tab displays a graph showing how QoS varied during the call. The horizontal scale and frequency of data points (dots on the lines of the graph) vary based on the length of the call. Hover over a data point to see the value at that point.

**Signaling Diagram** | This tab displays a diagram showing the sequence of signaling events during the call. The image lists signaling events from the endpoints, MCUs, and any RealPresence DMA system(s) involved in the call (more than one cluster may be represented if using a superclustered configuration). The header for each column is labeled with the device name, its IP address, and the signaling port. Click on a signaling message or call property change to view details about that message or property change. Each signaling message is labeled with the message time, sequence number, and message type. The sequence number matches the sequence number for the event in the call events tab. Click **Download Image** to save a copy of the call events diagram to your PC. Click **Download Call Events (XML)** to save the call event details in XML format. **Note:** Fully external calls, whose signaling does not pass through the RealPresence DMA system, have no signaling diagrams.
The Polycom RealPresence DMA system integrates with endpoint devices to support videoconferencing. You can monitor and manage endpoints from your system’s management interface.

- Monitor Endpoints
- Add an Endpoint
- Edit an Endpoint
- Edit Multiple Endpoints
- Add an Alias
- Edit an Alias
- Associate a User With a Device
- Disassociate a User From an Endpoint
- Block Registrations From an Endpoint
- Unblock Registrations From an Endpoint
- Quarantine an Endpoint
- Unquarantine an Endpoint
- Names and Aliases in a Mixed H.323 and SIP Environment
- Naming ITP Systems for Recognition by the Polycom RealPresence DMA System

### Monitor Endpoints

You can monitor endpoints based on various search criteria.

#### To monitor endpoints:

1. **Go to Monitoring > Endpoints.**
   - The search field above the list of endpoints lets you find devices matching the criteria you specify. The default search finds all endpoints with active registrations.
2. **To view all endpoints, regardless of registration status, click the filter button next to the Name field and turn off Registration status as one of the search criteria.**
3. **Click Search to display all endpoints.**
   - The following table describes the information that displays in the Endpoints list.
<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the device.</td>
</tr>
<tr>
<td>Model</td>
<td>The model designation of the device.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the device.</td>
</tr>
<tr>
<td>Alias</td>
<td>The aliases, if any, assigned to the device.</td>
</tr>
<tr>
<td>Site</td>
<td>The site to which the device belongs.</td>
</tr>
<tr>
<td>Owner Domain</td>
<td>The domain to which the device’s owner, if any, belongs.</td>
</tr>
<tr>
<td>Owner</td>
<td>The user who owns the device.</td>
</tr>
<tr>
<td>Class of Service</td>
<td>The class of service assigned to the device:</td>
</tr>
<tr>
<td></td>
<td>• Gold</td>
</tr>
<tr>
<td></td>
<td>• Silver</td>
</tr>
<tr>
<td></td>
<td>• Bronze</td>
</tr>
<tr>
<td></td>
<td>• Inherit from associated user (if none, default to Bronze)</td>
</tr>
<tr>
<td>Note:</td>
<td>The class of service of the device applies to point to point calls. VMR</td>
</tr>
<tr>
<td></td>
<td>calls use the class of service of the conference room.</td>
</tr>
<tr>
<td>Admission Policy</td>
<td>Indicates the admission policy applied to the device:</td>
</tr>
<tr>
<td></td>
<td>• Allow</td>
</tr>
<tr>
<td></td>
<td>• Block</td>
</tr>
<tr>
<td></td>
<td>• Quarantine</td>
</tr>
<tr>
<td></td>
<td>• Reject</td>
</tr>
<tr>
<td>Compliance Level</td>
<td>Indicates whether the device is compliant or non-compliant with the applicable registration policy script.</td>
</tr>
</tbody>
</table>
Endpoints

For more search options, click the filter button to the right of the Name field.

Select the filters you want and enter search strings for one or more fields.

Leave a filter’s field empty to match all values for that filter.

Click Search.

The system matches any string you enter against the beginning of the values for which you entered it. If you enter “10.33.17” in the IP address field, it displays devices whose IP addresses are in that subnet. To search for a string not at the beginning of the field, you can use an asterisk (*) as a wildcard.

The Actions list associated with the Endpoints list contains the items in the following table.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Details</td>
<td>Opens the Device Details dialog for the selected endpoint.</td>
</tr>
<tr>
<td>Add</td>
<td>Opens the Add Endpoint dialog, where you can manually add a device to the system.</td>
</tr>
</tbody>
</table>

Registration Status

The registration status of the device:

- **Active** – The device is registered and can make and receive calls.
- **Inactive** – The device’s registration has expired. Whether it can make and receive calls depends on the system’s rogue call policy in Call Server Settings.
- **Quarantined** – The device is registered, but it cannot make or receive calls. It remains in Quarantined or Quarantined (Inactive) status until you remove it from quarantine.
- **Quarantined (Inactive)** – The device was quarantined, and its registration has expired. It can register again, returning to Quarantined status.
- **Blocked** – The device is not permitted to register. It remains blocked from registering until you unblock it.

- If the device is in a site managed by the system, its ability to make and receive calls depends on the system’s rogue call policy.
- If the device is not in a site managed by the system, it can’t make or receive calls.

A device’s status can be determined by:

- An action by the device.
- An action applied to it manually on this page.
- The expiration of a timer.
- The application of a registration policy and admission policy.

Exceptions

Shows any exceptions returned for a device as a result of applying a registration policy script.

Active Calls

Indicates if the device is in a call.

Device Authentication

Indicates whether the endpoint must authenticate itself.

Note: Inbound authentication for the device type must be enabled at the system level, or the setting for the device has no effect.
Endpoints

Add an Endpoint

You can manually add an endpoint to the system. When you do so, the system applies its registration policy script (see Registration Policy) to determine the device’s compliance level (compliant or non-compliant with the policy), and then applies the admission policy associated with that result to determine the registration status of the device.

To add an endpoint:

1. Go to Monitoring > Endpoints.
2. Under Actions, click Add.
3. Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit</td>
<td>Opens the Edit Endpoint dialog for the selected endpoint, where you can change its information and settings. If multiple endpoints are selected, opens the Edit Endpoints dialog, where you can change the device authentication, permanent registration, and class of service settings.</td>
</tr>
<tr>
<td>Delete</td>
<td>Removes the registration of the selected endpoint(s) with the Call Server and deletes the endpoint(s) from the Polycom RealPresence DMA system. A dialog asks you to confirm. Unregistered endpoints are treated like rogue endpoints (see Call Server Settings). The device can register again.</td>
</tr>
<tr>
<td>Associate User</td>
<td>Opens the Associate User dialog for the selected endpoint, where you can associate this device with a user.</td>
</tr>
<tr>
<td>Disassociate User</td>
<td>Disassociates a user from a selected endpoint.</td>
</tr>
<tr>
<td>Block Registrations</td>
<td>Prevents the endpoint(s) from registering with the Call Server. A dialog asks you to confirm. When blocked endpoints are selected, this becomes Unblock Registrations. If a blocked device is in a site managed by the system, its ability to make and receive calls depends on the system's rogue call policy (see Call Server Settings). If the device is not in a site managed by the system, it can’t make or receive calls.</td>
</tr>
<tr>
<td>Quarantine</td>
<td>Prevents the endpoint(s) from making or receiving calls. A dialog asks you to confirm. When quarantined endpoints are selected, this becomes Unquarantine. Unlike a blocked endpoint, a quarantined endpoint is registered (or can register) with the Call Server.</td>
</tr>
<tr>
<td>View Call History</td>
<td>Takes you to Reports &gt; Call History and displays the call history for the selected endpoint.</td>
</tr>
<tr>
<td>View Registration History</td>
<td>Takes you to Reports &gt; Registration History and displays the registration history for the selected endpoint.</td>
</tr>
</tbody>
</table>
Edit an Endpoint

You can change a device’s class of service settings, add aliases, and edit or delete added aliases. You cannot edit or delete aliases with which the device registered.

To edit a device:

1. Go to Monitoring > Endpoints.
2. Enter the search criteria you want and click Search to display endpoints that match your criteria.
3. Select the device to edit.

4. Click OK.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device type</td>
<td>The device’s signaling protocol (H.323 or SIP).</td>
</tr>
<tr>
<td>Signaling address</td>
<td>For an H.323 device, the H.225 call signaling address and port of the device. Either this or the RAS address is required.</td>
</tr>
<tr>
<td>RAS address</td>
<td>For an H.323 device, the RAS (Registration, Admission and Status) channel address and port of the device.</td>
</tr>
<tr>
<td>Aliases</td>
<td>For an H.323 device, lists the device’s aliases. When you add a device, this list is empty. The Add button lets you add an alias.</td>
</tr>
<tr>
<td>Address of record</td>
<td>For a SIP device, the AOR with which the device registers (see registration rules in RFC 3261), such as: sip:<a href="mailto:1000@westminster.polycom.com">1000@westminster.polycom.com</a></td>
</tr>
<tr>
<td>Device authentication</td>
<td>Indicates whether the endpoint must authenticate itself.</td>
</tr>
<tr>
<td>Class of service</td>
<td>Select to specify the class of service and the bit rate limits for calls to and from this device.</td>
</tr>
<tr>
<td></td>
<td>A call between two devices receives the higher class of service of the two.</td>
</tr>
<tr>
<td></td>
<td>Note: The class of service of the device applies to point to point calls. VMR calls use the class of service of the conference room.</td>
</tr>
<tr>
<td>Maximum bit rate (kbps)</td>
<td>The maximum bit rate for calls to and from this device.</td>
</tr>
<tr>
<td>Minimum downspeed bit rate (kbps)</td>
<td>The minimum bit rate to which calls from this device can be downspeeded to manage bandwidth. If this minimum isn’t available, the call is dropped.</td>
</tr>
<tr>
<td>Model</td>
<td>Optional model number/name for the device.</td>
</tr>
<tr>
<td>Version</td>
<td>Optional version information for the device.</td>
</tr>
</tbody>
</table>
5 Revise the editable fields as needed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the H.323 or SIP device. For an H.323 device, the name is the Alias Value of the most-recently added alias. Display only.</td>
</tr>
<tr>
<td>Model</td>
<td>The model of the endpoint, if known. Display only.</td>
</tr>
<tr>
<td>Aliases</td>
<td>For an H.323 device, lists the device's aliases. When you edit a device, you can edit or delete an existing alias, or add a new alias.</td>
</tr>
<tr>
<td>Site</td>
<td>The site to which the device belongs. Display only.</td>
</tr>
<tr>
<td>Owner domain</td>
<td>The domain to which the device’s owner belongs, if provided by the device. Display only.</td>
</tr>
<tr>
<td>Owner</td>
<td>The user who owns the device, if provided by the device. Display only.</td>
</tr>
<tr>
<td>Registration status</td>
<td>The registration status of the device. Display only.</td>
</tr>
<tr>
<td>Permanent</td>
<td>When selected, prevents the registration from ever expiring.</td>
</tr>
<tr>
<td>Device authentication</td>
<td>Indicates whether the endpoint must authenticate itself. Note: Inbound authentication for the device type must be enabled at the system level, or the setting for the device has no effect.</td>
</tr>
<tr>
<td>Class of service</td>
<td>Select to modify the class of service and the bit rate limits for calls to and from this device. A call between two devices receives the higher class of service of the two. Note: The class of service of the device applies to point-to-point calls. VMR calls use the class of service of the conference room.</td>
</tr>
<tr>
<td>Maximum bit rate (kbps)</td>
<td>The maximum bit rate for calls to and from this device.</td>
</tr>
<tr>
<td>Minimum downspeed bit rate (kbps)</td>
<td>The minimum bit rate to which calls from this device can be downspeeded to manage bandwidth. If this minimum isn’t available, the call is dropped.</td>
</tr>
<tr>
<td>Forward if no answer</td>
<td>If the device doesn’t answer, forward calls to the specified alias. Registered endpoints can activate this feature by dialing the vertical service code (VSC) for it (default is *73) followed by the alias. They can deactivate it by dialing the VSC alone.</td>
</tr>
<tr>
<td>Forward if busy</td>
<td>If the device is busy, forward calls to the specified alias. Registered endpoints can activate this feature by dialing the VSC for it (default is *74) followed by the alias. They can deactivate it by dialing the VSC alone.</td>
</tr>
<tr>
<td>Forward unconditionally</td>
<td>Forward all calls to the specified alias. Registered endpoints can activate this feature by dialing the VSC for it (default is *75) followed by the alias. They can deactivate it by dialing the VSC alone.</td>
</tr>
<tr>
<td>Alert when endpoint unregisters</td>
<td>If the device unregisters from the Call Server or its registration expires, an informational alert is triggered (see Alert 5003).</td>
</tr>
</tbody>
</table>
Edit Multiple Endpoints

When you select multiple endpoints, you can change certain settings for all of the selected endpoints at one time.

To edit multiple endpoints:

1. Go to Monitoring > Endpoints.
2. Enter the search criteria you want and click Search to display endpoints that match your criteria.
3. Select the device to edit.
   - Use SHIFT-CLICK or CTRL-CLICK to select one or more additional endpoints.
5. Complete the fields in the Edit Endpoints window as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permanent</td>
<td>Prevents the registration of the selected devices from ever expiring.</td>
</tr>
<tr>
<td>Device authentication</td>
<td>Indicates whether the selected devices must authenticate themselves.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Inbound authentication for the device type must be enabled at the system level or the setting for these devices has no effect. See Device Authentication.</td>
</tr>
<tr>
<td>Class of service</td>
<td>Select to modify the class of service and the bit rate limits for calls to and from the selected devices.</td>
</tr>
<tr>
<td></td>
<td>A call between two devices receives the higher class of service of the two.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The class of service of the device applies to point to point calls. VMR calls use the class of service of the conference room.</td>
</tr>
<tr>
<td>Maximum bit rate (kbps)</td>
<td>The maximum bit rate for calls to and from the selected devices.</td>
</tr>
<tr>
<td>Minimum downspeed bit rate (kbps)</td>
<td>The minimum bit rate to which calls from the selected devices can be downspeeded to manage bandwidth. If this minimum isn't available, the call is dropped.</td>
</tr>
<tr>
<td>Alert when device unregisters</td>
<td>If one of the selected devices unregisters from the Call Server or its registration expires, an informational alert is triggered (see Alert 5003).</td>
</tr>
</tbody>
</table>

6. Click OK.

Delete an Endpoint

You can delete one or more inactive endpoints from the RealPresence DMA system. An inactive device is one whose registration has expired. Depending on your Registration Policy settings, inactive devices may be automatically deleted after a specified number of days.

To delete a device:

1. Go to Monitoring > Endpoints.
2. Enter the search criteria you want and click Search to display endpoints that match your criteria.
3. Select the device to delete.
4. Under Actions, click Delete.
5. Click Yes to confirm the deletion.

Add an Alias

You can specify an alias for an H.323 device that you add or edit.

To add an alias:
1. Go to Monitoring > Endpoints.
2. Do one of the following:
   - Under Actions, click Add.
   - Search for an endpoint, select it from the list and, under Actions, click Edit.
3. In the Aliases section, click the Add button.
4. Enter the alias in the Value field and click OK.

Edit an Alias

You can revise an existing alias that you have added for an H.323 device. You cannot edit an alias with which a device registered.

To edit an alias:
1. Go to Monitoring > Endpoints.
2. Search for and select the endpoint with the alias you want to edit.
4. In the Aliases section, select the alias to edit.
5. Click the Edit button.
6. Revise the alias in the Value field as needed and click OK.
7. Click OK to close the Edit Endpoint window.

Associate a User With a Device

You can associate an endpoint with a user by selecting the endpoint, then searching for the user with whom to associate it. You can search by First name, Last name, and/or User ID. The Search users field searches all three for matches.

Note that the system matches the string you enter against the beginning of the field you are searching. For example, if you enter "sa" in the Last name field, the search results display users whose last names begin with "sa." To search for a matching string not at the beginning of the field, you can use an asterisk (*) as a wildcard, such as "*sa".
To associate a user with a device:

1. Go to Monitoring > Endpoints.
2. Select the endpoint to associate with a user.
3. Under Actions, click Associate User.
4. Enter the search criteria you want and click Search to display users that match your criteria.
5. Select the user to associate with the endpoint and click OK.
6. Click Yes to confirm the association.

The Owner column on the Endpoints page displays the user associated with the endpoint.

Disassociate a User From an Endpoint

When necessary, you can disassociate a selected device from an associated user.

To disassociate a user from an endpoint:

1. Go to Monitoring > Endpoints.
2. Search for and select the endpoint to disassociate from a user.
4. Click Yes to confirm the disassociation.

Block Registrations From an Endpoint

Blocking a device prevents it from registering with the RealPresence DMA system.

To block registrations from a device:

1. Go to Monitoring > Endpoints.
2. Enter the search criteria you want and click Search to display endpoints that match your criteria.
3. Select the endpoint to block from registering with the RealPresence DMA system.
   ➢ Use SHIFT-CLICK or CTRL-CLICK to select one or more additional endpoints to block.
4. Under Actions, click Block Registrations.
5. Click Yes to confirm the block.

Unblock Registrations From an Endpoint

Unblocking a blocked device allows it to register with the RealPresence DMA system.

To unblock registrations from an Endpoint:

1. Go to Monitoring > Endpoints.
2. Enter the search criteria you want and click Search to display endpoints that match your criteria.
3. Select the endpoint to unblock from registering.
To unquarantine an endpoint:
1. Go to Monitoring > Endpoints.
2. Enter the search criteria you want and click Search to display endpoints that match your criteria.
3. Select the endpoint to unquarantine.
   ➢ Use Shift-click or Ctrl-click to select one or more additional endpoints to unquarantine.
4. Under Actions, click Unquarantine.
5. Click Yes to confirm the removal from quarantine.

Names and Aliases in a Mixed H.323 and SIP Environment

An endpoint that supports both H.323 and SIP can register with the Polycom RealPresence DMA system's gatekeeper and SIP registrar using the same name/alias. When the RealPresence DMA system receives a call for that endpoint, it uses the protocol of the calling endpoint. This can lead to failed calls under the following circumstances:

- The system is configured to allow calls to/from rogue (not actively registered) endpoints (see Configure the Call Server).
Endpoints

- An endpoint that was registered with both protocols (using the same name/alias) later has one of the protocols disabled, and that registration expires (or otherwise becomes inactive).

The RealPresence DMA system is not aware if an endpoint no longer supports a protocol. When another endpoint tries to call using the called endpoint’s disabled protocol, the system still tries to reach it using that protocol, and the call fails.

To avoid this problem, you can do one of the following:

- Ensure that endpoints supporting both protocols use different names/aliases for each protocol.
- Do not allow calls to/from rogue endpoints.
- If you know an endpoint has stopped supporting a protocol, manually delete its inactive registration for that protocol.

Naming ITP Systems for Recognition by the Polycom RealPresence DMA System

A Polycom Immersive Telepresence (ITP) room system contains multiple displays and codecs (endpoints). If the ITP system is using SIP or H.323 signaling (not Cisco TIP signaling), the Polycom RealPresence DMA system will recognize the endpoints as part of an ITP system only if they have names that properly identify them. The names must take the form systemName_M_N, where M is the total number of displays in the ITP system (2, 3, or 4) and N is the sequence number of each display. The “primary” codec must be assigned sequence number 1.

For example, the three HDX devices in a Polycom OTX 300 ITP system named Bainbridge might be named as follows:

- Bainbridge ITP_3_1
- Bainbridge ITP_3_2
- Bainbridge ITP_3_3

When these three devices register with the Polycom RealPresence DMA system’s Call Server, the RealPresence DMA system recognizes them as a single ITP system and assigns them a Gold class of service (you can change this if necessary). The RealPresence DMA system also manages the device authentication settings as applying to a single system.

For ITP systems using SIP or TIP signaling (but not H.323), the RealPresence DMA system also creates a single CDR for calls from the ITP system rather than separate CDRs for each of the three devices.

You can only edit the device authentication and class of service settings for the primary codec; the RealPresence DMA system automatically propagates any changes to the other devices in the ITP system.

The RealPresence DMA system’s ability to recognize ITP calls and treat them as one assures the same class of service and device authentication settings for all the endpoints in the ITP system, but not other registration settings. You need to ensure that the maximum and minimum bit rates and other registration settings are consistent.

Follow this naming convention for both the ITP system name and the name for each HDX endpoint in the ITP system. For more information, see the following documents:

- Administrator’s Guide for Polycom HDX Systems
- Polycom Immersive Telepresence (ITP) Deployment Guide
- Polycom Multipoint Layout Application (MLA) User’s Guide for Use with Polycom Telepresence Solutions
### High Availability Status

If you have RealPresence DMA systems configured in High Availability (HA) mode, you can monitor the status of the HA pair from the management user interface.

### Monitor High Availability Status

You can monitor the status of an HA pair, including network connections, virtual IP address activity, and connection status of the local node.

#### To monitor High Availability status:

2. The following HA status information displays:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Status</strong></td>
<td></td>
</tr>
<tr>
<td>High Availability</td>
<td>Specifies if High Availability mode is enabled or disabled.</td>
</tr>
<tr>
<td>Local connection</td>
<td>Indicates whether the local node is connected to the network on all interfaces that have services (and therefore a virtual IP address) assigned.</td>
</tr>
<tr>
<td>Peer connection</td>
<td>Indicates whether the peer node is connected to the network on all interfaces that have services (and therefore a virtual IP address) assigned.</td>
</tr>
<tr>
<td><strong>Virtual IP Address List</strong></td>
<td></td>
</tr>
<tr>
<td>Virtual IP</td>
<td>Each of the virtual IP addresses configured for the HA pair.</td>
</tr>
<tr>
<td>Address Active</td>
<td>Specifies whether the virtual IP address is active on one of the two HA nodes (Yes or No).</td>
</tr>
<tr>
<td>Active Locally</td>
<td>Specifies whether the virtual IP address is active on the local node (Yes); if No, the virtual IP address is active on the peer node.</td>
</tr>
<tr>
<td><strong>Local HA Service Status</strong></td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td>Each network interface on the local node that’s configured for HA communication with the peer.</td>
</tr>
</tbody>
</table>
## High Availability Status

**Interface Status**
Specifies whether the interface has a working connection to the network (Up) or is not connected to the network (Down).

**Local HA Service Status**
Indicates whether the interface has a connection to the HA communication channel (Active or Inactive).
Note that although a connection may exist, the local node and the peer may not actually be communicating (e.g., the peer might be unreachable, but the local node is still Active because it's capable of communicating with the peer).

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Status</td>
<td>Specifies whether the interface has a working connection to the network (Up) or is not connected to the network (Down).</td>
</tr>
<tr>
<td>Local HA Service Status</td>
<td>Indicates whether the interface has a connection to the HA communication channel (Active or Inactive). Note that although a connection may exist, the local node and the peer may not actually be communicating (e.g., the peer might be unreachable, but the local node is still Active because it's capable of communicating with the peer).</td>
</tr>
</tbody>
</table>
Login Sessions

You can view all active user login sessions on your Polycom® RealPresence® DMA® system. If you are an Administrator user, you can terminate login sessions when necessary.

View Login Sessions

You can monitor all active login sessions on your RealPresence DMA system.

To view login sessions:

» Go to Monitoring > Login Sessions.

The following table describes the parts of the Login Sessions list.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain/User Name</td>
<td>The domain to which the user belongs.</td>
</tr>
<tr>
<td>Client Platform</td>
<td>The platform from which the user logged in.</td>
</tr>
<tr>
<td>Client Address</td>
<td>The IP address from which the user logged in.</td>
</tr>
<tr>
<td>Host Name</td>
<td>The length of the session in minutes.</td>
</tr>
<tr>
<td>Creation Time</td>
<td>The time and date when the user logged in.</td>
</tr>
</tbody>
</table>

Terminate a User’s Login Session

You can terminate a user’s login session manually in the Login Sessions page.

To terminate a user’s login session

1. Go to Monitoring > Login Sessions.
2. In the Login Sessions list, select the login session you want to terminate.
3. Under Actions, click Terminate Session.
4. Click Yes to confirm.
   - The system terminates the session immediately and informs the user that the connection to the server was lost.
Site Statistics

The **Site Statistics** page lists the sites defined in the Polycom RealPresence DMA system’s site topology and, for those controlled by the system, traffic and QoS statistics. Network clouds and the default Internet site are not included.

The following table describes the fields in the list.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Name</td>
<td>Name of the site.</td>
</tr>
<tr>
<td>Number of Calls</td>
<td>Number of active calls on this site.</td>
</tr>
<tr>
<td>Bandwidth Used %</td>
<td>Percentage of available bandwidth in use for this site.</td>
</tr>
<tr>
<td>Bandwidth (bps)</td>
<td>Total bandwidth in use for this site.</td>
</tr>
<tr>
<td></td>
<td>Note: The value of the <strong>Bit rate to bandwidth conversion factor</strong> setting is used to calculate the bandwidth in use.</td>
</tr>
<tr>
<td>Avg Bit Rate (bps)</td>
<td>Average bit rate of this site’s active calls.</td>
</tr>
<tr>
<td></td>
<td>Note: The value of the <strong>Bit rate to bandwidth conversion factor</strong> setting is used to calculate the average bit rate.</td>
</tr>
<tr>
<td>Packet Loss %</td>
<td>Average packet loss percentage of this site’s active calls.</td>
</tr>
<tr>
<td>Avg Jitter (msec)</td>
<td>Average jitter rate of this site’s active calls.</td>
</tr>
<tr>
<td>Avg Delay (msec)</td>
<td>Average delay rate of this site’s active calls.</td>
</tr>
<tr>
<td>Territory</td>
<td>Territory to which the site belongs.</td>
</tr>
<tr>
<td>Cluster</td>
<td>Cluster responsible for the territory to which the site belongs.</td>
</tr>
</tbody>
</table>
Site Link Statistics

The Site Link Statistics page lists the site links defined in the Polycom RealPresence DMA system’s site topology and for those controlled by the system, traffic and QoS statistics.

The following table describes the fields in the list.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Name</td>
<td>Name of the site.</td>
</tr>
<tr>
<td>Number of Calls</td>
<td>Number of active calls on this site.</td>
</tr>
<tr>
<td>Bandwidth Used %</td>
<td>Percentage of available bandwidth in use for this site.</td>
</tr>
<tr>
<td>Bandwidth (bps)</td>
<td>Total bandwidth in use for this site.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: The value of the Bit rate to bandwidth conversion factor setting is used to calculate the bandwidth in use.</td>
</tr>
<tr>
<td>Avg Bit Rate (bps)</td>
<td>Average bit rate of this site’s active calls.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: The value of the Bit rate to bandwidth conversion factor setting is used to calculate the average bit rate.</td>
</tr>
<tr>
<td>Packet Loss %</td>
<td>Average packet loss percentage of this site’s active calls.</td>
</tr>
<tr>
<td>Avg Jitter (msec)</td>
<td>Average jitter rate of this site’s active calls.</td>
</tr>
<tr>
<td>Avg Delay (msec)</td>
<td>Average delay rate of this site’s active calls.</td>
</tr>
<tr>
<td>Territory</td>
<td>Territory to which the site belongs.</td>
</tr>
<tr>
<td>Cluster</td>
<td>Cluster responsible for the territory to which the site belongs.</td>
</tr>
</tbody>
</table>
SNMP Monitoring

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of resources in a network.

SNMP Framework

The SNMP framework has three parts:

- **An SNMP manager**
  The SNMP manager is the system used to control and monitor the activities of network hosts using SNMP. A variety of network management applications are available for use with SNMP. You should understand how your SNMP management system is configured to properly configure your RealPresence DMA system SNMP requirements, including transport protocol, version, authentication, and privacy. For information on using SNMP management systems, see the appropriate documentation for your application.

- **An SNMP agent**
  The SNMP agent is the software component within the RealPresence DMA system that maintains the data for the system and reports the data, as needed, to managing systems. The agent and MIB reside on the same system.

- **A MIB**
  The MIB (Management Information Base) is a virtual information storage area for network management information, which consists of collections of managed network objects. You can configure the SNMP agent for a particular system MIB. The agent gathers data from the MIB, the repository for information about system parameters and network data. Polycom systems include Polycom-specific MIBs as well as third-party MIBs. Polycom MIBs are self-documenting, including information about the purpose of specific traps and inform notifications. Third-party MIBs accessible through the Polycom system may include both hardware and software system MIBs.

SNMP Versions

Polycom supports two versions of SNMP:

- **SNMPv2c**—Polycom implements a sub-version of SNMPv2. SNMPv2c uses a community-based form of security. The community of SNMP managers able to access the agent MIB is defined by an IP-based Access Control List and password.
  
  SNMPv2c does not encrypt communications between the management system and SNMP agents and is subject to packet sniffing of the clear text community string from the network traffic.
SNMP Monitoring

- **SNMPv3**—SNMPv3 provides secure access to systems by authenticating and encrypting packets over the network. The `contextEngineID` in SNMPv3 uniquely identifies each SNMP entity. The `contextEngineID` is used to generate the key for authenticated messages. Polycom implements SNMPv3 communication with authentication and privacy (the authPriv security level as defined in the USM MIB).
  - Authentication is used to ensure that traps are read by only the intended recipient. As messages are created, they are given a special key that is based on the `contextEngineID` of the entity. The key is shared with the intended recipient and used to receive the message.
  - Privacy encrypts the SNMP message to ensure that it cannot be read by unauthorized users.
  - Message integrity ensures that a packet has not been tampered with in transit.

**SNMP Notifications**

A key feature of SNMP is the ability to generate notifications from an SNMP agent. The RealPresence DMA system sends notifications, unsolicited and asynchronous, to the SNMP manager. Notifications can indicate improper user authentication, restarts, the closing of a connection, loss of connection to another system, or other significant events. They are generated as inform or trap requests.

Traps are messages alerting the SNMP manager to a system or network condition change. Informs are traps that include a request for a confirmation receipt from the SNMP manager. Traps are less reliable than informs because the SNMP manager does not send any acknowledgment when it receives a trap. However, informs consume more system and network resources. Traps are discarded as soon as they are sent. An inform request is held in memory until a response is received or the request times out. Traps are sent only once while informs may be retried several times. The retries increase traffic and contribute to a higher overhead on the network. Thus, traps and informs provide a trade-off between reliability and network resources.

**Configure SNMP Settings**

Configure the RealPresence DMA SNMP Agent Setting first, then add security users and notification listeners as needed.

**To configure SNMP settings:**

1. Go to **Admin > Server > SNMP Settings**.
2. Select **Enable SNMP monitoring**.
3 Configure the following settings for the connection between the RealPresence DMA system and the SNMP agent.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Version</td>
<td>Specifies the version of SNMP you want to use.</td>
</tr>
<tr>
<td>v2c</td>
<td>Used for standard models. Uses community-based authentication.</td>
</tr>
<tr>
<td>v3</td>
<td>Used when you want a high security model. Requires a security user for notifications.</td>
</tr>
<tr>
<td>Transport</td>
<td>Specifies the transport protocol for SNMP communications.</td>
</tr>
<tr>
<td>TCP</td>
<td>This protocol has error-recovery services, message delivery is assured, and</td>
</tr>
<tr>
<td></td>
<td>messages are delivered in the order they were sent. Some SNMP managers only</td>
</tr>
<tr>
<td></td>
<td>support SNMP over TCP.</td>
</tr>
<tr>
<td>UDP</td>
<td>This protocol does not provide error-recovery services, message delivery is</td>
</tr>
<tr>
<td></td>
<td>not assured, and messages are not necessarily delivered in the order they</td>
</tr>
<tr>
<td></td>
<td>were sent.                     Because UDP does not have error recovery services, it requires fewer network</td>
</tr>
<tr>
<td></td>
<td>resources. It is well suited for repetitive, low-priority functions like alarm monitoring.</td>
</tr>
<tr>
<td>Port</td>
<td>Specifies the port that the RealPresence DMA system uses to send SNMP</td>
</tr>
<tr>
<td></td>
<td>messages. Default port is 161 for UDP or TCP.</td>
</tr>
<tr>
<td>Community</td>
<td>For SNMPv2c, specifies the context for the information, which is the SNMP</td>
</tr>
<tr>
<td></td>
<td>group to which the devices and management stations running SNMP belong.</td>
</tr>
<tr>
<td></td>
<td>The RealPresence DMA system uses only the public context and will not</td>
</tr>
<tr>
<td></td>
<td>respond to requests from management systems that do not belong to its community.</td>
</tr>
<tr>
<td>Contact</td>
<td>The contact information for the SNMP agent. This may be a name, role, or</td>
</tr>
<tr>
<td></td>
<td>other identifying information.</td>
</tr>
<tr>
<td>Location</td>
<td>The physical location of the RealPresence DMA system.</td>
</tr>
<tr>
<td>Local engine ID</td>
<td>For SNMPv3 only. Displays the RealPresence DMA system contextEngineID for SNMPv3.</td>
</tr>
<tr>
<td>Security user</td>
<td>For SNMPv3 only. Specifies the security name required to access a monitored MIB object. This name cannot be &quot;snmpuser.&quot;</td>
</tr>
</tbody>
</table>

4 Click **Update**.

**Notification Settings**

In **Notification Settings**, you can specify the notification listeners (agents) and the types of notifications an agent sends to the RealPresence DMA system.
Add a Notification Listener

A notification listener sends SNMP messages to the RealPresence DMA system. To limit the effect on system performance, you can add a maximum of eight notification listeners.

To add a notification listener:

1. Go to Admin > SNMP Settings > Notification Settings.
2. Click the add button.
3. In the Add Notification Listener window, configure the settings as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable agent</td>
<td>Select to enable the notification listener. Clear to stop using this agent without deleting it.</td>
</tr>
<tr>
<td>Transport</td>
<td>The transport protocol for SNMP communications from the listening agent. (TCP or UDP).</td>
</tr>
<tr>
<td>Address</td>
<td>The IP address of the listening agent that sends SNMP notifications to the RealPresence DMA system.</td>
</tr>
<tr>
<td>Port</td>
<td>The port that the listening agent uses to send notifications to the RealPresence DMA system. Default port is 162 for UDP or TCP.</td>
</tr>
</tbody>
</table>
| Notification type | The type of notification that this listening agent sends to the RealPresence DMA system:  
  - Inform—The agent sends an unsolicited message to a notification receiver and expects or requires the receiver to respond with a confirmation message.  
  - Trap—The agent sends an unsolicited message to a notification receiver and does not expect or require a confirmation message. |
| SNMP version   | The version of SNMP used by this agent (v2c or v3). |
| Security user  | For SNMP v3, the user name of the security user authorized to actively retrieve SNMP data. |

4. Click OK.

The notification listener displays in the Notification Settings list.

5. Select the Minimum recurring notification interval from the drop-down list.

6. Click Update to save the settings.

Edit a Notification Listener

Revise notification listeners as needed when settings change.

To edit a notification agent:

1. Go to Admin > SNMP Settings.
2. From the Notification Settings list, select the notification listener to edit and click the edit button.
3. Revise the settings in the Edit Notification Listener window as needed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable agent</td>
<td>Select to enable the notification listener. Clear to stop using this agent without deleting it.</td>
</tr>
<tr>
<td>Transport</td>
<td>The transport protocol for SNMP communications from the listening agent. (TCP or UDP).</td>
</tr>
<tr>
<td>Address</td>
<td>The IP address of the listening agent that sends SNMP notifications to the RealPresence DMA system.</td>
</tr>
<tr>
<td>Port</td>
<td>The port that the listening agent uses to send notifications to the RealPresence DMA system. Default port is 162 for UDP or TCP.</td>
</tr>
<tr>
<td>Notification type</td>
<td>The type of notification that this listening agent sends to the RealPresence DMA system:</td>
</tr>
<tr>
<td>SNMP version</td>
<td>The version of SNMP used by this agent (v2c or v3).</td>
</tr>
<tr>
<td>Security user</td>
<td>For SNMP v3, the user name of the security user authorized to actively retrieve SNMP data.</td>
</tr>
</tbody>
</table>

4. Click OK to save the changes.
5. Select the Minimum recurring notification interval from the drop-down list.
6. Click Update to save the settings.

**Delete a Notification Listener**
Delete notification listeners if they are no longer valid.

**To delete a notification listener:**
1. Go to Admin > SNMP Settings > Notification Setting.
2. Select the agent to delete and click the delete button.
3. Click Yes to confirm the deletion.
4. Click Update to save your changes.

**Security Users**
Security users or clients are authorized to receive notifications (traps or informs) sent to the RealPresence DMA system.
Add a Security User

For SNMPv3 notifications, you must specify at least one security user.

To add a security user:

1. Go to Admin > Server > SNMP Settings.
2. Under Security User, click the add button.
3. In the Add Security User window, configure the following settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security user</td>
<td>The user name of the security user authorized to actively retrieve SNMP data.</td>
</tr>
<tr>
<td>Authentication type</td>
<td>The authentication protocol used to create unique fixed-sized message digests of a variable length message.</td>
</tr>
<tr>
<td></td>
<td>• MD5–Creates a digest of 128 bits (16 bytes)</td>
</tr>
<tr>
<td></td>
<td>• SHA–Creates a digest of 160 bits (20 bytes)</td>
</tr>
<tr>
<td></td>
<td>Both methods include the authentication key with the SNMPv3 packet and then generate a digest of the entire SNMPv3 packet.</td>
</tr>
<tr>
<td></td>
<td>The RealPresence DMA system implements communication with authentication and privacy (the authPriv security level, as defined in the USM MIB).</td>
</tr>
<tr>
<td>Authentication password</td>
<td>The authentication password that is used, together with the local engine ID, to create the authentication key included in the MD5 or SHA message digest.</td>
</tr>
<tr>
<td>Confirm password</td>
<td></td>
</tr>
<tr>
<td>Encryption type</td>
<td>The privacy protocol for the connection between the RealPresence DMA system and the SNMP agent.</td>
</tr>
<tr>
<td></td>
<td>• DES–Uses a 56-bit key with a 56-bit salt to encrypt the SNMPv3 packet</td>
</tr>
<tr>
<td></td>
<td>• AES–Uses a 128-bit key with a 128-bit salt to encrypt the SNMPv3 packet</td>
</tr>
<tr>
<td>Encryption password</td>
<td>The password that the privacy protocol uses, together with the local engine ID, to create the encryption key.</td>
</tr>
<tr>
<td>Confirm password</td>
<td></td>
</tr>
</tbody>
</table>

4. Click OK.
   The user displays in the Security User list.
5. Click Update to save the settings.

Edit a Security User

The settings for a security user can be revised as needed.


To edit a security user:

1. Go to Admin > Server > SNMP Settings.
2. In the Security User list, select the user to edit.
3. Click the edit button.
4. In the **Edit Security User** window, revise the following settings as needed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security user</td>
<td>The user name of the security user authorized to actively retrieve SNMP data.</td>
</tr>
</tbody>
</table>
| Authentication type     | The authentication protocol used to create unique fixed-sized message digests of a variable length message.  
  • MD5—Creates a digest of 128 bits (16 bytes)  
  • SHA—Creates a digest of 160 bits (20 bytes)  
  Both methods include the authentication key with the SNMPv3 packet and then generate a digest of the entire SNMPv3 packet.  
  The RealPresence DMA system implements communication with authentication and privacy (the authPriv security level, as defined in the USM MIB).|
| Authentication password | The authentication password that is used, together with the local engine ID, to create the authentication key included in the MD5 or SHA message digest. |
| Confirm password        |                                                                            |
| Encryption type         | The privacy protocol for the connection between the RealPresence DMA system and the SNMP agent.  
  • DES—Uses a 56-bit key with a 56-bit salt to encrypt the SNMPv3 packet  
  • AES—Uses a 128-bit key with a 128-bit salt to encrypt the SNMPv3 packet|
| Encryption password     | The password that the privacy protocol uses, together with the local engine ID, to create the encryption key. |
| Confirm password        |                                                                            |

5. Click **OK**.

6. Click **Update** to save the settings.

**Delete a Security User**

Delete security users when you no longer want them to receive SNMP notifications.

**To delete a security user:**

1. Go to **Admin > Server > SNMP Settings**.
2. In the **Security User** list, select the user to delete.
3. Click the delete button.
4. Click **Yes** to confirm the deletion.
5. Click **Update** to save your changes.
Download MIBs

The following MIBs are available from the RealPresence DMA system. You can download any of them from the SNMP Settings page.

Polycom recommends that you view MIB files with a MIB viewer application.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIB-Dell-10892</td>
<td>The hardware-specific MIB.</td>
</tr>
<tr>
<td>POLYCOM-BASE-MIB</td>
<td>The base MIB for Polycom products.</td>
</tr>
<tr>
<td>POLYCOM-DMA-MIB</td>
<td>The RealPresence DMA system-specific MIB definition.</td>
</tr>
<tr>
<td>POLYCOM-MCU-MANAGEMENT</td>
<td>The Polycom MCU MIB that contains MCU-related information, including MCU states.</td>
</tr>
<tr>
<td>RFC1213-MIB</td>
<td>The MIB for TCP/IP network management.</td>
</tr>
<tr>
<td>SNMPv2-CONF</td>
<td>A definition file for standard conventions included for reference.</td>
</tr>
<tr>
<td>SNMPv2-SMI</td>
<td>A definition file for standard conventions included for reference.</td>
</tr>
<tr>
<td>SNMPv2-TC</td>
<td>A definition file for standard conventions included for reference.</td>
</tr>
</tbody>
</table>

To download a MIB:

1. Go to Admin > SNMP Settings.
2. Click Download MIBs.
3. Select the MIB and click Download.
4. Save or open the MIB file locally.
5. Click OK to close the Download DMA MIBS window.
Reports

This section provides an introduction to using and configuring Polycom® RealPresence® DMA® system reports. It includes:

- Alert History
- Call History
- Conference History
- Registration History
- Call Detail Records
- Orphaned Groups and Users
- Conference Room Errors Report
- Enterprise Passcode Errors Report
- Network Usage Report
System Reports

The Polycom® RealPresence® DMA® system provides the following reports:

- Alert History
- Call History
- Conference History
- Registration History
- Call Detail Records
- Network Usage Report

Alert History

You can view all the system alerts for the time period you select. The system retains the most recent 500 alerts. Each alert includes the start and end time, alert code, and description.

To view alert history:

1. Go to Reports > Alert History.
2. Use the search pane above the list as follows to find alerts matching the criteria you specify:
   - Click the filter icon to expand the search pane.
   - Select the appropriate filter to search by description, alert code, or time period.
3. Click Search to display the results.

Call History

You can view detailed records of calls and download call detail records (CDRs). The records include point-to-point calls through Call Server and VMR calls through Conference Manager.

You can search for calls by dial string and limit your search by specifying one or more of the following:

- Originator device’s name, alias, or IP address
- Destination device’s name, alias, or IP address
- Signaling type used in the call (H.323, SIP, WebRTC)
- Registration status of the call originator
- Cluster, territory, or site
To view call history:

1. Go to Reports > Call History.
2. Use the search pane above the list as follows to find calls matching the criteria you specify:
   - Click the filter icon to expand the search pane.
   - Select the appropriate filter to narrow your search results.
3. Click Search to display the following information:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Originator</td>
<td>The originating device’s display name, name, alias, or IP address (in that order of preference), depending on what it provided in the call signaling. If the originator is an MCU, the MCU name.</td>
</tr>
<tr>
<td>Dial String</td>
<td>Dial string sent by originator, when available.</td>
</tr>
<tr>
<td>Destination</td>
<td>The destination device’s display name, name, alias, or IP address (in that order of preference), depending on what it provided in the call signaling. If the destination is an MCU, the MCU name; if a VSC, the VSC value (not including the VSC).</td>
</tr>
<tr>
<td>Start Time</td>
<td>Time the call began (first signaling event).</td>
</tr>
<tr>
<td>End Time</td>
<td>Time the call ended (session closed).</td>
</tr>
<tr>
<td>Ingress Cluster</td>
<td>The cluster (the first, if more than one) that handled the call.</td>
</tr>
<tr>
<td>Call ID</td>
<td>Unique identifier for the call.</td>
</tr>
</tbody>
</table>

**Export Search Results**

The Export Search Results command lets you download just the records displayed on the page (the current search results). A Save dialog prompts you to select a location for the downloaded file. The default filename is CDRSearchExport.tar. This is a troubleshooting feature. To aid in resolving a problem, Polycom Global Services may ask you to use specific search criteria to retrieve certain call records, download them, and send the file to them for analysis of the records.

**Show Export History**

The Export History list provides a record of the CDR exports and search results exported from the system. The list includes the following fields:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>User ID of the person who performed the export.</td>
</tr>
<tr>
<td>Export Type</td>
<td>One of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>CDR</strong> for CDR exports</td>
</tr>
<tr>
<td></td>
<td>• <strong>Call History</strong> for search results exports</td>
</tr>
</tbody>
</table>
The Export History list is the same on the Call History and Conference History pages. In both places, all export operations are shown.

To view export history:

1. Go to Reports > Call History or Conference History.
2. Search for calls or conferences based on the criteria you need to match.
3. Under Actions, click Show Export History.
   The Export History list displays below the list of search results.

Hide Export History

You can hide the Export History list from the Call History or Conference History page when necessary.

To hide export history:

1. Go to Reports > Call History or Conference History.
2. Search for calls or conferences based on the criteria you need to match.
3. Under Actions, click Show Export History.
   The Export History list displays below the list of search results.
4. When you finish viewing the Export History, click Hide Export History.

Show Call Details

Call details provide specific information about any call you select from the list of calls.

To view call details:

1. Go to Reports > Call History.
2. Search for calls based on the criteria you need to match.
3. Select a call from the list of search results and click Show Call Details.
   The Call Details window displays.
4. Select from the categories on the left side of the window to display related details.

Conference History

The Conference History page lets you view detailed records of conferences and download CDRs (call detail records).
The fields at the top of the page let you specify the starting and ending date and time or the conference ID for which you want to view conference records.

When setting the date/time range for your search, keep in mind that retrieving a large number of records can take some time.

After you search for conferences, the Conference History page lists all the conferences in the time range you specified. If there are more than 500, the first page lists the first 500, and the arrow buttons below the list let you view other pages. The following table describes the fields in the list.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conference Room ID</td>
<td>The conference room ID.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Time the conference began (first conference event).</td>
</tr>
<tr>
<td>End Time</td>
<td>Time the conference ended (last conference event).</td>
</tr>
<tr>
<td>Cluster</td>
<td>The cluster that handled the conference.</td>
</tr>
</tbody>
</table>

**Show Export History**

The Export History list provides a record of the CDR exports and search results exported from the system. The list includes the following fields:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>User ID of the person who performed the export.</td>
</tr>
<tr>
<td>Export Type</td>
<td>One of the following:</td>
</tr>
<tr>
<td></td>
<td>• CDR for CDR exports</td>
</tr>
<tr>
<td></td>
<td>• Call History for search results exports</td>
</tr>
<tr>
<td>Date of Export</td>
<td>Date and time of the export.</td>
</tr>
<tr>
<td>Cluster</td>
<td>The cluster from which the export took place.</td>
</tr>
</tbody>
</table>

The Export History list is the same on the Call History and Conference History pages. In both places, all export operations are shown.

**To view export history:**

1. Go to Reports > Call History or Conference History.
2. Search for calls or conferences based on the criteria you need to match.
3. Under Actions, click Show Export History. The Export History list displays below the list of search results.

**Hide Export History**

You can hide the Export History list from the Call History or Conference History page when necessary.
To hide export history:
1. Go to Reports > Call History or Conference History.
2. Search for calls or conferences based on the criteria you need to match.
3. Under Actions, click Show Export History.
   The Export History list displays below the list of search results.
4. When you finish viewing the Export History, click Hide Export History.

Associated Calls
The Associated Calls list shows all the calls associated with the selected conference. The following table describes the fields in the list.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call ID</td>
<td>Unique identifier for the call.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Time the call began (first signaling event).</td>
</tr>
<tr>
<td>End Time</td>
<td>Time the call ended (session closed).</td>
</tr>
<tr>
<td>Originator</td>
<td>The originating device's display name, name, alias, or IP address (in that order of preference), depending on what it provided in the call signaling. If the originator is an MCU, the MCU name.</td>
</tr>
<tr>
<td>Destination</td>
<td>The destination device's display name, name, alias, or IP address (in that order of preference), depending on what it provided in the call signaling. If the destination is an MCU, the MCU name; if a VSC, the VSC value (not including the VSC).</td>
</tr>
<tr>
<td>Cluster</td>
<td>The cluster (first, if more than one) that handled the call.</td>
</tr>
</tbody>
</table>

The Display Call History command (in the Actions list) takes you to the Call History page and displays the call that was selected in the Associated Calls list.

Conference Events
The Conference Events list provides much more detail about the selected conference, listing every state change and call event in the course of the conference. The following table describes the fields in the list.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the event.</td>
</tr>
<tr>
<td>Attributes</td>
<td>Information about the event (varies with the event type).</td>
</tr>
<tr>
<td>Call UUID</td>
<td>Call identifier (if call event).</td>
</tr>
<tr>
<td>Time</td>
<td>Date and time of the event.</td>
</tr>
<tr>
<td>Sequence</td>
<td>Identifies when in the order of changes to this conference this event occurred.</td>
</tr>
</tbody>
</table>
When you select a conference event with a call UUID, the Display Call History command (in the Actions list) takes you to the Call History page and displays the associated call.

Property Changes

The Property Changes list provides more information about the selected conference, listing every change in the value of a conference property during the course of the conference. The following table describes the fields in the list.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the call property.</td>
</tr>
<tr>
<td>Value</td>
<td>Value assigned to the property.</td>
</tr>
<tr>
<td>Time</td>
<td>Date and time of the property change.</td>
</tr>
<tr>
<td>Sequence</td>
<td>Identifies when in the order of changes to this call this property change occurred.</td>
</tr>
</tbody>
</table>

Registration History

Registration History provides access to information about registered devices. It also provides information about external SIP peers with which the system is registered, if any.

View the Registration History

When the call server is providing H.323 gatekeeper or SIP registrar services, you can view information about registered devices.

To view registration history:

1. Go to Reports > Registration History.

The following fields display in the registrations list:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the registered device.</td>
</tr>
<tr>
<td>Alias</td>
<td>The device’s alias.</td>
</tr>
<tr>
<td>Start Time</td>
<td>The time and date that the device registered.</td>
</tr>
</tbody>
</table>
Use the search pane above the list as follows to find registrations matching the criteria you specify:

- Click the filter icon to expand the search pane.
- Select the appropriate filter to search by alias or IP address.

Limit your search as needed by specifying one or more of the following:

- Owner, territory, or site
- Signaling protocol (H.323 or SIP)
- Registration status
- Device type (endpoint or gateway)

Click **Search**.

The registrations that match your search criteria display below the search fields.

Under **Actions**, click **Show Details** to display the **Registration Details** and the **Events and Signaling Messages** tabs below the list, enabling you to see:

- Detailed information about the selected device’s registration status and information.
- A history of the registration signaling and processing, including the results of applying the registration policy script, if any.

### Call Detail Records

In addition to the online call and conference history reports, the Polycom RealPresence DMA system generates call detail records (CDRs) for all calls and conferences, which you can download.

After you unzip the download file, you can open the two CSV files it contains (one for calls and one for conferences) with Microsoft Excel or another spreadsheet application. The CSV files contain a line for each call or conference that ended during the selected time frame.

The ZIP file also includes a text file that contains a single line specifying:

- The number of calls in the call CDR file.
- The number conferences in the conference CDR file.
- The clusters whose calls and conferences are included in the CDR file.
- The clusters whose calls and conferences are excluded from the CDR file because those clusters were not reachable when the CDR export was generated.
Caution: Only one CDR should be generated at a time. If you run a client application that issues API calls to automatically generate and download CDRs at the same time that you manually attempt to generate and download a CDR, you or the client application may receive errors.

Export CDR Data

From the Call History or Conference History page, you can use the Export CDR Data command to download call detail records for the time period you specify.

To export CDRs:

1. Go to Reports > Call History (or Conference History).
2. Under Actions, click Export CDR Data.
3. In the Export Time Frame dialog, set the Calls and conferences ending after date and time and the Calls and conferences ending before date and time as the parameters for your CDR data query.
   - The defaults provide all CDR data for the current day. Times and dates are in the time zone of your browser.
4. Click OK.
   - The system displays the progress as it gathers the information needed to construct the CDR data files.
5. When the Exporting CDR Data dialog displays Data has been prepared and is ready to be downloaded, click Download to select a location for the downloaded file. The default filename is cdrExport.zip, but you can rename it.
6. Choose a path and filename for the CDR file and click Save.
   - The Exporting CDR Data dialog shows the progress.
7. When the download is complete, click Close.

Call Record Layouts

The following table describes the fields in the call detail records.

Times and dates in the CDR file are expressed in the time zone of the RealPresence DMA cluster that created the CDR export, with the GMT offset shown at the end. Note that if a conference spans a daylight savings time change, the offset for endTime will be different from the offset for startTime.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>version</td>
<td>Changes each time the format of CDRs changes.</td>
</tr>
<tr>
<td>type</td>
<td>CALL</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>callType</td>
<td>One of the following:</td>
</tr>
<tr>
<td></td>
<td>• PT-PT</td>
</tr>
<tr>
<td></td>
<td>• VMR</td>
</tr>
<tr>
<td></td>
<td>• VEQ</td>
</tr>
<tr>
<td></td>
<td>• VSC-hunt group</td>
</tr>
<tr>
<td></td>
<td>• VSC-{uncond fwd</td>
</tr>
<tr>
<td></td>
<td>• VMR-subscribe only</td>
</tr>
<tr>
<td></td>
<td>• VMR-Lync AVMCU</td>
</tr>
<tr>
<td>callUuid</td>
<td>Unique identifier for the call.</td>
</tr>
<tr>
<td>dialin</td>
<td>If this is point-to-point or a VMR dial-in call, TRUE. Otherwise, FALSE.</td>
</tr>
<tr>
<td>startTime</td>
<td>YYYY-MM-DDTHH:MM:SS.FFF[+</td>
</tr>
<tr>
<td></td>
<td>(ISO 8601 syntax, where FFF is milliseconds and Z is zero offset)</td>
</tr>
<tr>
<td></td>
<td>This is when call signaling reached the RealPresence DMA system, not when</td>
</tr>
<tr>
<td></td>
<td>media started. If multiple call records, the start of this segment of the call.</td>
</tr>
<tr>
<td>endTime</td>
<td>YYYY-MM-DDTHH:MM:SS.FFF[+</td>
</tr>
<tr>
<td></td>
<td>(ISO 8601 syntax, where FFF is milliseconds and Z is zero offset)</td>
</tr>
<tr>
<td></td>
<td>This is when the RealPresence DMA system’s involvement with the call ended,</td>
</tr>
<tr>
<td></td>
<td>not when media ended. If multiple call records, the end of this segment of</td>
</tr>
<tr>
<td></td>
<td>the call.</td>
</tr>
<tr>
<td>origEndpoint</td>
<td>The originating endpoint's display name, name, alias, or IP address (in that</td>
</tr>
<tr>
<td></td>
<td>order of preference), depending on what it provided in the call signaling.</td>
</tr>
<tr>
<td></td>
<td>If the originator is an MCU, the MCU name.</td>
</tr>
<tr>
<td>dialString</td>
<td>Initial dial string as supplied by the originator. If multiple call records,</td>
</tr>
<tr>
<td></td>
<td>this value is the same across all segments of the call.</td>
</tr>
<tr>
<td>destEndpoint</td>
<td>The destination endpoint's display name, name, alias, or IP address (in that</td>
</tr>
<tr>
<td></td>
<td>order of preference), depending on what it provided in the call signaling.</td>
</tr>
<tr>
<td></td>
<td>If the destination is an MCU, the MCU name; if a VSC, the VSC value (not</td>
</tr>
<tr>
<td></td>
<td>including the VSC character).</td>
</tr>
<tr>
<td>origSignalType</td>
<td>One of the following:</td>
</tr>
<tr>
<td></td>
<td>• h323</td>
</tr>
<tr>
<td></td>
<td>• sip</td>
</tr>
<tr>
<td>destSignalType</td>
<td>One of the following:</td>
</tr>
<tr>
<td></td>
<td>• h323</td>
</tr>
<tr>
<td></td>
<td>• sip</td>
</tr>
<tr>
<td>refConfUUID</td>
<td>If VMR call, confUUID of the associated conference.</td>
</tr>
<tr>
<td>lastForwardEndpoint</td>
<td>If call forwarding, endpoint that forwarded call to the final destination endpoint.</td>
</tr>
<tr>
<td>cause</td>
<td>Cause value for call termination or termination of this CDR. This may not be</td>
</tr>
<tr>
<td></td>
<td>the end of the call.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>causeSource</td>
<td>Source of the termination of the call record. Indicates which participant requested call disconnect:</td>
</tr>
<tr>
<td></td>
<td>• originator</td>
</tr>
<tr>
<td></td>
<td>• destination</td>
</tr>
<tr>
<td></td>
<td>• callserver</td>
</tr>
<tr>
<td>bitRate</td>
<td>Bit rate for call, in kbps. If the bit rate changes during the call, this is a list of bit rate values separated by plus signs (+). For instance:</td>
</tr>
<tr>
<td></td>
<td>1024+768+384</td>
</tr>
<tr>
<td>classOfService</td>
<td>Class of service for the call:</td>
</tr>
<tr>
<td></td>
<td>• Gold</td>
</tr>
<tr>
<td></td>
<td>• Silver</td>
</tr>
<tr>
<td></td>
<td>• Bronze</td>
</tr>
<tr>
<td>ingressCluster</td>
<td>The RealPresence DMA cluster of the originating endpoint or entry point from a neighbor or SBC.</td>
</tr>
<tr>
<td>egressCluster</td>
<td>The RealPresence DMA cluster of the destination endpoint or exit point to a neighbor or SBC.</td>
</tr>
<tr>
<td>VMRCluster</td>
<td>The RealPresence DMA cluster handling the VMR, or blank if not a VMR call.</td>
</tr>
<tr>
<td>VEQCluster</td>
<td>The RealPresence DMA cluster handling the VEQ, or blank if no VEQ.</td>
</tr>
<tr>
<td>userRole</td>
<td>If VMR call, the role of the caller in conference:</td>
</tr>
<tr>
<td></td>
<td>• PARTICIPANT</td>
</tr>
<tr>
<td></td>
<td>• CHAIRPERSON (entered passcode)</td>
</tr>
<tr>
<td></td>
<td>Null if not VMR call.</td>
</tr>
<tr>
<td>userDataA</td>
<td>The value from the User pass-through to CDR field of the user associated with the endpoint. For point-to-point calls, this is the user associated with the endpoint that started this call.</td>
</tr>
<tr>
<td>userDataB</td>
<td>For VMR calls, the value from the Conference room pass-through to CDR field of the conference room (VMR) to which the call connected. For point-to-point calls, the value from the User pass-through to CDR field of the user associated with the endpoint that received this call.</td>
</tr>
<tr>
<td>userDataC</td>
<td>For VMR calls, the dial-out participant pass-through value provided via the API, if any. For point-to-point calls, not currently used.</td>
</tr>
<tr>
<td>userDataD</td>
<td>Not currently used.</td>
</tr>
<tr>
<td>userDataE</td>
<td>Not currently used.</td>
</tr>
<tr>
<td>failureSignalingCode</td>
<td>For SIP calls, the SIP code and reason, separated by a colon, that the call was disconnected. For instance:</td>
</tr>
<tr>
<td></td>
<td>486:BUSY HERE</td>
</tr>
<tr>
<td>origModel</td>
<td>The hardware model of the originating device, if available from the device’s registration or other signaling.</td>
</tr>
</tbody>
</table>

System Reports
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>origVersion</td>
<td>The software version of the originating device, if available from the device’s registration or other signaling.</td>
</tr>
<tr>
<td>destModel</td>
<td>The hardware model of the destination device, if available from the device’s registration or other signaling.</td>
</tr>
<tr>
<td>destVersion</td>
<td>The software version of the destination device, if available from the device’s registration or other signaling.</td>
</tr>
<tr>
<td>displays</td>
<td>For an immersive telepresence room, the number of screens the room has. For a Polycom SIP ITP call, this is determined from the system name; for a Polycom or Cisco TIP call, it’s the <code>x-cisco-multiple-screen</code> parameter value. For all other calls, the value is 1. <strong>Note:</strong> If a Polycom ITP room doesn’t follow the ITP naming convention, this field may contain inaccurate information.</td>
</tr>
<tr>
<td>minVideoResolution</td>
<td>The minimum vertical resolution used on the video channel, followed by the minimum frame rate while at the minimum resolution, as reported by the MCU at the end of the call. For instance: 480p15. Zero (0) if the call was audio only. Available only for AVC calls using SIP or TIP signaling to a version 8.1 or newer hardware-based Polycom MCU with MPMx cards. Otherwise, blank.</td>
</tr>
<tr>
<td>maxVideoResolution</td>
<td>The maximum vertical resolution used on the video channel, followed by the maximum frame rate while at the maximum resolution, as reported by the MCU at the end of the call. For instance: 720p30. Zero (0) if the call was audio only. Available only for AVC calls using SIP or TIP signaling to a version 8.1 or newer hardware-based Polycom MCU with MPMx cards. Otherwise, blank.</td>
</tr>
<tr>
<td>videoPeakJitter</td>
<td>The peak jitter (in milliseconds) on the video channel. Zero (0) if the call was audio only. Available only for AVC calls using SIP or TIP signaling to a version 8.1 or newer hardware-based Polycom MCU with MPMx cards. Otherwise, blank.</td>
</tr>
<tr>
<td>videoTotalPackets</td>
<td>The total number of packets sent on the video channel. Zero (0) if the call was audio only. Available only for AVC calls using SIP or TIP signaling to a version 8.1 or newer hardware-based Polycom MCU with MPMx cards. Otherwise, blank.</td>
</tr>
<tr>
<td>videoTotalLostPackets</td>
<td>The number of packets lost on the video channel. Zero (0) if the call was audio only. Available only for AVC calls using SIP or TIP signaling to a version 8.1 or newer hardware-based Polycom MCU with MPMx cards. Otherwise, blank.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>minContentResolution</td>
<td>The minimum vertical resolution used on the content channel, followed by the minimum frame rate while at the minimum resolution, as reported by the MCU at the end of the call. Zero (0) if content was not shared. Available only for AVC calls using SIP or TIP signaling to a version 8.1 or newer hardware-based Polycom MCU with MPMx cards. Otherwise, blank.</td>
</tr>
<tr>
<td>maxContentResolution</td>
<td>The maximum vertical resolution used on the content channel, followed by the maximum frame rate while at the maximum resolution, as reported by the MCU at the end of the call. Zero (0) if content was not shared. Available only for AVC calls using SIP or TIP signaling to a version 8.1 or newer hardware-based Polycom MCU with MPMx cards. Otherwise, blank.</td>
</tr>
<tr>
<td>contentPeakJitter</td>
<td>The peak jitter (in milliseconds) on the content channel. Zero (0) if content was not shared. Available only for AVC calls using SIP or TIP signaling to a version 8.1 or newer hardware-based Polycom MCU with MPMx cards. Otherwise, blank.</td>
</tr>
<tr>
<td>contentTotalPackets</td>
<td>The total number of packets sent on the content channel. Zero (0) if content was not shared. Available only for AVC calls using SIP or TIP signaling to a version 8.1 or newer hardware-based Polycom MCU with MPMx cards. Otherwise, blank.</td>
</tr>
<tr>
<td>contentTotalLostPackets</td>
<td>The number of packets lost on the content channel. Zero (0) if content was not shared. Available only for AVC calls using SIP or TIP signaling to a version 8.1 or newer hardware-based Polycom MCU with MPMx cards. Otherwise, blank.</td>
</tr>
<tr>
<td>origSignalingId</td>
<td>For SIP point-to-point or VMR calls (dialin=TRUE), the complete From header of the INVITE received from the endpoint. For VMR SIP dial-outs (dialin=FALSE), the To header sent by the RealPresence DMA system to the MCU. Otherwise, blank.</td>
</tr>
<tr>
<td>origCallId</td>
<td>The SIP or H.323 call ID of the call between the originating endpoint and the RealPresence DMA system. For VMR dial-outs, the call ID of the call between the RealPresence DMA system and the MCU.</td>
</tr>
<tr>
<td>destCallId</td>
<td>The SIP or H.323 call ID of the call between the destination endpoint and the RealPresence DMA system. For calls to a VMR, the call ID of the call between the RealPresence DMA system and the MCU.</td>
</tr>
<tr>
<td>chairPasscode</td>
<td>The configured chairperson passcode for the conference room. Blank if no passcode was configured at the time of the conference.</td>
</tr>
<tr>
<td>confRequiresChair</td>
<td>TRUE if the conference template used for the conference has the Conference requires chairperson flag enabled. Otherwise, FALSE.</td>
</tr>
<tr>
<td>termConfAfterChairDrops</td>
<td>TRUE if the conference template used for the conference has the Terminate conference after chairperson drops flag enabled. Otherwise, FALSE.</td>
</tr>
<tr>
<td>charJoinTime</td>
<td>The time the first chairperson joined the conference. If no chairperson joined the conference, blank.</td>
</tr>
</tbody>
</table>
## Conference Record Layouts

The following table describes the fields in the conference records.

Times and dates in the CDR file are expressed in the time zone of the RealPresence DMA cluster that created the CDR export, with the GMT offset shown at the end. Note that if a conference spans a daylight savings time change, the offset for `endTime` will be different from the offset for `startTime`.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>version</td>
<td>Changes each time the format of CDRs changes.</td>
</tr>
<tr>
<td>type</td>
<td>CONF</td>
</tr>
<tr>
<td>confType</td>
<td>One of the following:</td>
</tr>
<tr>
<td></td>
<td>• PCO — for Polycom Conferencing for Outlook (calendared) conferences</td>
</tr>
<tr>
<td></td>
<td>• LYNC — for Lync conferences</td>
</tr>
<tr>
<td></td>
<td>• AD-HOC — for all other conferences</td>
</tr>
<tr>
<td>cluster</td>
<td>The RealPresence DMA cluster serving the VMR.</td>
</tr>
<tr>
<td>confUUID</td>
<td>Unique identifier for the conference.</td>
</tr>
<tr>
<td>startTime</td>
<td>`YYYY-MM-DDTHH:MM:SS.FFF[+</td>
</tr>
<tr>
<td></td>
<td>(ISO 8601 syntax, where FFF is milliseconds and Z is zero offset)</td>
</tr>
<tr>
<td></td>
<td>This is when the first participant joined the conference.</td>
</tr>
<tr>
<td>endTime</td>
<td>`YYYY-MM-DDTHH:MM:SS.FFF[+</td>
</tr>
<tr>
<td></td>
<td>(ISO 8601 syntax, where FFF is milliseconds and Z is zero offset)</td>
</tr>
<tr>
<td></td>
<td>This is when the last participant left the conference.</td>
</tr>
<tr>
<td>userID</td>
<td>Conference room (VMR) owner, shown as:</td>
</tr>
<tr>
<td></td>
<td>• domain\user</td>
</tr>
<tr>
<td></td>
<td>Domain is LOCAL for non-AD users.</td>
</tr>
<tr>
<td></td>
<td>If this is a Lync conference, this field is empty.</td>
</tr>
<tr>
<td>roomID</td>
<td>Conference room (VMR) number or Lync conference ID.</td>
</tr>
<tr>
<td>partCount</td>
<td>Maximum number of concurrent calls in the conference (high water mark).</td>
</tr>
<tr>
<td></td>
<td>Doesn’t include audio-only IVR dial-outs or participants dialed directly</td>
</tr>
<tr>
<td></td>
<td>into or out from the MCU without going through the RealPresence DMA system.</td>
</tr>
<tr>
<td></td>
<td>The following are counted as a single participant:</td>
</tr>
<tr>
<td></td>
<td>• A Polycom or Cisco immersive telepresence room using Cisco TIP signaling.</td>
</tr>
<tr>
<td></td>
<td>• A Polycom ITP room using SIP signaling and the prescribed naming</td>
</tr>
<tr>
<td></td>
<td>convention.</td>
</tr>
<tr>
<td>classOfService</td>
<td>Class of service for the call:</td>
</tr>
<tr>
<td></td>
<td>• Gold</td>
</tr>
<tr>
<td></td>
<td>• Silver</td>
</tr>
<tr>
<td></td>
<td>• Bronze</td>
</tr>
<tr>
<td>userDataA</td>
<td>The value from the User pass-through to CDR field of the user associated</td>
</tr>
<tr>
<td></td>
<td>with the conference room (VMR).</td>
</tr>
</tbody>
</table>
Network Usage Report

The Network Usage page displays historical usage data about the video network. You can export the network usage data as a CSV (comma-separated values) file.
Use the search feature to select the network usage criteria to include in the report:

- Start time and span/granularity data
- Cluster, territory, or throttlepoint (site, site link, or subnet) data
- Specific call, QoS, and bandwidth data

The data matching the criteria you choose displays as a graph.

**Export Network Usage Data**

You can download a CSV (comma-separated values) file containing all the network usage data point records for the time period you specify.

The system retains the most recent 8 million data points.

**To export network usage data:**

1. Go to Monitoring > Network Usage.
2. Enter the following search criteria as needed:
   - Time granularities
   - Start time
   - Type
   - Value
3. Click **Search** to display specific call, QoS, and bandwidth data you want to see.
4. Click **Export Network Usage**.
5. Set the **Export Time Frame Start Date** and time and the **Export Time Frame End Date** and time you want to include.
   - The default values provide all network usage data for the past 24 hours.
6. Click **OK**.
7. Choose a path and filename for the network usage file and click **Save**.
8. When the download is complete, click **Close**.
   - You can open the CSV file with Microsoft Excel or another spreadsheet application.

**View Network Usage Data**

When you export network usage data, the file includes a network usage data point record for each throttlepoint, territory, and cluster for each minute of the time period you specified for the report. It does not include usage data for MPLS clouds, the default Internet site, or sites not controlled by the system.

The following table describes the fields in the records.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Name of the throttlepoint, territory, or cluster that defines the scope being measured.</td>
</tr>
<tr>
<td>date</td>
<td>Minutes since 1970 (Java time / 60,000).</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>calls_started</td>
<td>Number of calls started in the scope during the time interval.</td>
</tr>
<tr>
<td>callsEnded</td>
<td>Number of calls ended in the scope during the time interval.</td>
</tr>
<tr>
<td>calls_dropped</td>
<td>Number of calls rejected or evicted due to bandwidth limits at the throttlepoint during the time interval. The calls dropped measure is intended to help with understanding network congestion. So, it includes calls dropped due to available bandwidth at the throttlepoint, but not calls dropped due to per call bitrate limits at the throttlepoint.</td>
</tr>
<tr>
<td>calls_downs speeded</td>
<td>Number of calls downspeeded due to bandwidth limits at the throttlepoint during the time interval. The calls downspeeded measure is intended to help with understanding network congestion. So, it includes calls downspeeded due to available bandwidth at the throttlepoint, but not calls downspeeded due to per call bitrate limits at the throttlepoint.</td>
</tr>
<tr>
<td>bitrate_limit</td>
<td>The (maximum) configured bitrate limit for the scope during the time interval, or -1 if no limit was configured (kbps).</td>
</tr>
<tr>
<td>bandwidth_limit</td>
<td>The (maximum) configured bandwidth limit for the scope during the time interval, or -1 if no limit was configured (kbps).</td>
</tr>
<tr>
<td>bandwidth_usage</td>
<td>The (maximum) used bandwidth for the scope during the time interval (kbps).</td>
</tr>
<tr>
<td>bandwidth_usage_percent</td>
<td>The (maximum) percentage of the bandwidth limit used for the scope during the time interval (kbps).</td>
</tr>
<tr>
<td>packet_loss_percent</td>
<td>Mean packet loss percentage of all QoS reports in the scope during the time interval.</td>
</tr>
<tr>
<td>avg_video_jitter</td>
<td>Mean jitter of all QoS reports of all video channels in the scope during the time interval (milliseconds).</td>
</tr>
<tr>
<td>max_video_jitter</td>
<td>Maximum jitter of all QoS reports of all video channels in the scope during the time interval (milliseconds).</td>
</tr>
<tr>
<td>avg_video_delay</td>
<td>Mean delay of all QoS reports of all video channels in the scope during the time interval (milliseconds).</td>
</tr>
<tr>
<td>max_video_delay</td>
<td>Maximum delay of all QoS reports of all video channels in the scope during the time interval (milliseconds).</td>
</tr>
<tr>
<td>avg_audio_jitter</td>
<td>Mean jitter of all QoS reports of all audio channels in the scope during the time interval (milliseconds).</td>
</tr>
<tr>
<td>max_audio_jitter</td>
<td>Maximum jitter of all QoS reports of all audio channels in the scope during the time interval (milliseconds).</td>
</tr>
<tr>
<td>avg_audio_delay</td>
<td>Mean delay of all QoS reports of all audio channels in the scope during the time interval (milliseconds).</td>
</tr>
<tr>
<td>max_audio_delay</td>
<td>Maximum delay of all QoS reports of all audio channels in the scope during the time interval (milliseconds).</td>
</tr>
<tr>
<td>gold_calls</td>
<td>Max concurrent Gold class calls in the scope during the time interval.</td>
</tr>
<tr>
<td>silver_calls</td>
<td>Max concurrent Silver class calls in the scope during the time interval.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>bronze_calls</td>
<td>Max concurrent Bronze class calls in the scope during the time interval.</td>
</tr>
<tr>
<td>audio_calls</td>
<td>Max concurrent audio calls in the scope during the time interval.</td>
</tr>
<tr>
<td>calls_256Kbps</td>
<td>Max concurrent video calls with a bitrate less than or equal to 320kbps in the scope during the time interval.</td>
</tr>
<tr>
<td>calls_384Kbps</td>
<td>Max concurrent video calls with a bitrate greater than 320kbps and less than or equal to 448kbps in the scope during the time interval.</td>
</tr>
<tr>
<td>calls_512Kbps</td>
<td>Max concurrent video calls with a bitrate greater than 448kbps and less than or equal to 640kbps in the scope during the time interval.</td>
</tr>
<tr>
<td>calls_768Kbps</td>
<td>Max concurrent video calls with a bitrate greater than 640kbps and less than or equal to 896kbps in the scope during the time interval.</td>
</tr>
<tr>
<td>calls_1Mbps</td>
<td>Max concurrent video calls with a bitrate greater than 896kbps and less than or equal to 1.5Mbps in the scope during the time interval.</td>
</tr>
<tr>
<td>calls_2Mbps</td>
<td>Max concurrent video calls with a bitrate greater than 1.5Mbps and less than or equal to 3Mbps in the scope during the time interval.</td>
</tr>
<tr>
<td>calls_4Mbps</td>
<td>Max concurrent video calls with a bitrate greater than 3Mbps in the scope during the time interval.</td>
</tr>
<tr>
<td>sip_calls</td>
<td>Max concurrent calls using SIP signaling in the scope during the time interval.</td>
</tr>
<tr>
<td>h323_calls</td>
<td>Max concurrent calls using H.323 signaling in the scope during the time interval.</td>
</tr>
<tr>
<td>gateway_calls</td>
<td>Max concurrent calls using the SIP to H.323 gateway in the scope during the time interval.</td>
</tr>
<tr>
<td>conference_calls</td>
<td>Max concurrent Conference Manager calls in the scope during the time interval.</td>
</tr>
</tbody>
</table>
Conference Room Errors Report

If the Polycom RealPresence DMA system is integrated with your Active Directory, it can create a conference room (virtual meeting room) for each enterprise user.

The Polycom RealPresence DMA system reads the Active Directory daily to refresh the information in its cache. It also rereads the directory whenever you update the directory integration settings.

If the directory integration settings are configured to generate conference room IDs for enterprise users, the Polycom RealPresence DMA system retrieves the values from the designated directory attribute and removes the specified characters from them. If the resulting room ID is longer than the specified maximum, it strips the excess characters from the beginning of the string.

The Conference Room Errors page reports the conference room ID generation status and lists the problem IDs.

You must be an enterprise user (with the appropriate user role assignments) to see the conference room errors report. A local user cannot access this page, regardless of user roles.

The summary at the top of the report shows when it was generated (check this to verify that the report you are viewing reflects the most recent update of the cache) and the following information:

- Total number of users found
- Number of users with valid conference room IDs
  If you do not specify a directory attribute from which to generate conference room IDs, this number is zero and the report contains nothing else of value.
- Number of users for whom the Active Directory field being used to generate conference room IDs is empty (these are counted, but not listed individually below; find them in the Active Directory).
- Number of users with blank conference room IDs (doesn’t include those for whom the Active Directory field was empty, only those for whom its contents were filtered out)
- Number of users with invalid conference room IDs
- Number of users with duplicate conference room IDs

The blank, invalid, and duplicate conference room IDs are listed below.

Duplicate conference room IDs are not disabled; they can be used for conferencing. But if both users associated with that conference room ID try to hold a conference at the same time, they end up in the same conference.

The following table describes the fields in the list.
Export Conference Room Errors Data

You can use the Export Room Errors Report command to download a CSV (comma-separated values) file containing all the data in the conference room errors report.

To export conference room errors data:

1. Go to Reports > Conference Room Errors.
2. In the Actions list, click Export Room Errors Report.
3. In the Exporting Conference Room Errors Report dialog, click Download.
4. Choose a path and filename for the file and click Save.
   The File Download dialog shows the progress.
5. When the download is complete, click Close.

You can open the CSV file with Microsoft Excel or another spreadsheet application. The file contains the same data you see displayed on the Conference Room Errors page.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problem</td>
<td>Description of the issue with this room ID (Blank, Duplicate, or Invalid).</td>
</tr>
<tr>
<td>Conference Room ID</td>
<td>The conference room ID, typically generated from the enterprise user’s phone number.</td>
</tr>
<tr>
<td>&lt;directory attribute&gt;</td>
<td>The attribute (field) from the Active Directory that’s used to generate the room ID. The column heading is the name of the attribute, such as telephoneNumber.</td>
</tr>
<tr>
<td>User ID</td>
<td>The login name or ID of the enterprise user with this room ID.</td>
</tr>
<tr>
<td>Domain</td>
<td>The domain to which the enterprise user belongs.</td>
</tr>
<tr>
<td>Last Name</td>
<td>The enterprise user’s last name.</td>
</tr>
<tr>
<td>First Name</td>
<td>The enterprise user’s first name.</td>
</tr>
<tr>
<td>Notes</td>
<td>For duplicates, identifies the domain and user ID of the user with a duplicate conference room ID.</td>
</tr>
</tbody>
</table>
Enterprise Passcode Errors Report

If the Polycom RealPresence DMA system is integrated with your Active Directory, conference and chairperson passcodes for enterprise users can be maintained in the Active Directory.

The Polycom RealPresence DMA system reads the Active Directory daily to refresh the information in its cache. It also rereads the directory whenever you update the directory integration settings (Integrations > Microsoft Active Directory).

If the directory integration settings are configured to generate passcodes for enterprise users, the Polycom RealPresence DMA system retrieves the values from the designated directory attributes and removes any non-numeric characters from them. If the resulting numeric passcode is longer than the specified maximum for that passcode type, it strips the excess characters from the beginning of the string.

The Enterprise Passcode Errors page reports the passcode generation status and lists the users with passcode errors.

You must be an enterprise user (with the appropriate user role assignments) to see the enterprise passcode errors report. A local user cannot access this page, regardless of user roles.

The summary at the top of the report shows when it was generated (check this to verify that the report you're viewing reflects the most recent update of the cache), the directory server accessed, and the following information:

- Number of users in the directory
- Number of users with duplicate chairperson and conference passcodes; for users with duplicate passcodes, the system ignores the conference passcode, but honors the chairperson passcode
- Number of users with valid, invalid, and unassigned chairperson passcodes and the directory attribute on which they are based, along with the number of users with locally overridden chairperson passcodes
- Number of users with valid, invalid, and unassigned conference passcodes and the directory attribute on which they are based, along with the number of users with locally overridden conference passcodes

The users with invalid passcodes are listed below. The following table describes the fields in the list.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problem</td>
<td>Indicates what the problem is: Chairperson, Conference, or Duplicate.</td>
</tr>
<tr>
<td>User ID</td>
<td>The login name or ID of the enterprise user with this passcode error.</td>
</tr>
<tr>
<td>Domain</td>
<td>The domain to which the enterprise user belongs.</td>
</tr>
<tr>
<td>Last Name</td>
<td>The enterprise user's last name.</td>
</tr>
</tbody>
</table>
Export Enterprise Passcode Errors Data

You can use the Export Enterprise Passcode Errors Report command to download a CSV (comma-separated values) file containing all the data in the enterprise passcode errors report.

To export enterprise passcode errors data:

1. Go to Reports > Enterprise Passcode Errors.
2. In the Actions list, click Export Enterprise Passcode Errors Report.
3. In the Exporting Enterprise Passcode Errors Report dialog, click Download.
4. Choose a path and filename for the file and click Save.
   The File Download dialog shows the progress.
5. When the download is complete, click Close.

You can open the CSV file with Microsoft Excel or another spreadsheet application. The file contains the same data you see displayed on the Enterprise Passcode Errors page.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Name</td>
<td>The enterprise user’s first name.</td>
</tr>
<tr>
<td>Notes</td>
<td>For an invalid passcode, shows the generated value (after the system stripped non-numeric characters out of the attribute value and truncated it if necessary). For duplicate chairperson and conference passcodes, shows the raw attribute value of each and the duplicate value generated (after stripping non-numeric characters and truncating if necessary).</td>
</tr>
</tbody>
</table>
Troubleshooting

This section provides an introduction to troubleshooting in the Polycom® RealPresence® DMA® system. It includes:

- System Log Files
- Alerts
- Troubleshooting Utilities
Alerts

On various pages and Dashboard panes, the alert icon is used to indicate an abnormal condition, problem, or just something you should be aware of. Hover over the icon to see details.

A summary of alert status appears in the menu bar, showing how many alerts exist across all clusters of a supercluster and how many are new (that is, that you have not viewed yet).

When you click the summary data, an expanded alerts list appears, displaying the date and time, alert code, and description of each alert. In many cases, the alert description is a link to the relevant page for investigating the issue. A Help button to the right of the alert description displays the help topic for that alert, which contains additional information about the causes and recommendations for dealing with the alert.

The following topics describe the alerts by category, followed by the alerts contained in the category:

- **Supercluster Status** (1000 series)
- **Territory Status** (1100 series)
- **Asynchronous Operation** (1200 series)
- **RealPresence Resource Manager System Integration** (2000 series)
- **Active Directory Integration** (2100 series)
- **Exchange Server Integration** (2200 series)
- **Database Status** (2400 series)
- **Skype for Business Integration** (2600 series)
- **Signaling** (3000 series)
- **Certificate** (3100 series)
- **Licenses** (3200 series)
- **Networks** (3300 series)
- **Server Resources** (3400 series)
- **Data Synchronization** (3600 series)
- **System Health and Availability** (3800 series)
- **Cluster Features** (3900 series)
- **MCUs** (4000 series)
- **Endpoints** (5000 series)
- **Conference Manager** (6000 series)
- **Conference Status** (6100 series)
- **Skype for Business Presence Publishing** (6200 series)
- **Call Server** (7000 series)
- **Call Bandwidth Management** (7100 series)
**Supercluster Status**

The following alerts provide information on changes in cluster and supercluster status.

**Alert 1001**

*Cluster <cluster> is busied out as of YYYY-MM-DD HH:MM GMT+/-H[::MM].*

You or another administrator busied out the cluster, perhaps for maintenance.

A busied-out cluster allows existing calls and conferences to continue and accepts new calls for existing conferences, but does not accept other new calls and conferences.

Once all existing calls and conferences have ended, the cluster is out of service.

Click the link to go to the DMAs page.

**Alert 1002**

*Cluster <cluster> is out of service as of YYYY-MM-DD HH:MM GMT+/-H[::MM].*

You or another administrator took the cluster out of service (or busied out the cluster, and now all calls and conferences have ended).

An out-of-service cluster is still running and accessible via the management interface, but does not accept any calls or registrations.

Click the link to go to the DMAs page.

**Alert 1003**

*Cluster <cluster> is orphaned.*

The replication link with the specified cluster seems to be corrupted.

Click the link to go to the DMAs page. Try removing that cluster from the supercluster and then rejoining.

**Alert 1004**

*Cluster <cluster> is not reachable. Last heartbeat received YYYY-MM-DD HH:MM GMT+/-H[::MM].*

The specified cluster is not sending scheduled heartbeats. Possible reasons include:

- The cluster may simply be very busy and have fallen behind in sending heartbeats.
- An internal process could be stuck.
- The servers may be offline or rebooting.
- There may be a network problem.

Click the link to go to the DMAs page.
**Territory Status**

The following alerts provide information on changes in territory status.

**Alert 1103**

*No clusters assigned to <list of territories>.*

The specified territory or territories are not assigned to a cluster, so any responsibilities assigned to the territories are not being fulfilled.

Click the link to go to the Territories page. Assign a primary and backup cluster for every territory in your site topology.

**Alert 1105**

*<alerting-cluster>: Primary cluster <p-cluster> and backup cluster <b-cluster> are not reachable. Territory <territory> may not be functioning.*

The cluster from which the alert originated is unable to communicate with the specified territory’s primary and backup clusters.

This may be a temporary problem, in which case this alert will be cleared as soon as the alerting cluster is once again able to communicate with the clusters in question.

If this alert reoccurs frequently but quickly goes away, that suggests intermittent spurious network problems. If it persists for more than about 15-30 seconds, it may indicate serious network problems. It is also possible that someone shut both clusters down, or shut down one and the other then failed, or both failed (unlikely).

Click the link to go to the Territories page. To enable conferencing to continue in the territory (at diminished capacity), assign it to some other cluster.

**Alert 1106**

*<alerting-cluster>: Cluster <cluster> is not reachable. Territory <territory> may not be functioning.*

The cluster from which the alert originated is unable to communicate with the specified territory’s primary cluster, and there is no backup cluster.

This may be a temporary problem, in which case this alert will be cleared as soon as the alerting cluster is once again able to communicate with the cluster in question.

If this alert reoccurs frequently but quickly goes away, that suggests intermittent spurious network problems. If it persists for more than about 15-30 seconds, it may indicate serious network problems. It is also possible that someone shut the cluster down or that it failed.

Click the link to go to the Territories page. To enable conferencing to continue in the territory (at diminished capacity), assign it to some other cluster.

We recommend assigning a backup cluster for each territory.
Alert 1107

>alerting-cluster>: Primary cluster <p-cluster> associated with territory <territory> is not reachable. But backup cluster <b-cluster> is reachable.

The cluster from which the alert originated is unable to communicate with the specified territory’s primary cluster, but can communicate with the backup cluster.

This may be a temporary problem, in which case this alert will be cleared as soon as the alerting cluster is once again able to communicate with the cluster in question.

If this alert reoccurs frequently but quickly goes away, that suggests intermittent network problems. If it persists, it will be followed by Alert 1108, indicating that the territory has failed over to the backup cluster.

The backup cluster allows conferencing to continue in the territory (at diminished capacity) and fulfills any other responsibilities assigned to the territory.

Click the link to go to the Territories page. Determine whether the cluster was deliberately shut down. If not, try pinging the cluster's IP addresses.

If this is a two-server cluster, and you cannot ping either the virtual or physical IP addresses, look for a network problem. It is unlikely that both servers have failed simultaneously.

If you can ping the cluster, the OS is running, but the application may be in a bad state. Try rebooting the servers.

Alert 1108

>alerting-cluster>: Territory <territory> has failed over from <p-cluster> to <b-cluster>.

The territory’s primary cluster is unreachable, and its backup cluster has taken over.

This may indicate a network problem. It is also possible that someone shut the cluster down or that it failed.

The backup cluster allows conferencing to continue in the territory (at diminished capacity) and fulfills any other responsibilities assigned to the territory.

Click the link to go to the Territories page. Determine whether the cluster was deliberately shut down. If not, try pinging the cluster’s IP addresses.

If this is a two-server cluster, and you can’t ping either the virtual or physical IP addresses, look for a network problem. It’s unlikely that both servers have failed simultaneously.

If you can ping the cluster, the OS is running, but the application may be in a bad state. Try rebooting the servers.

Asynchronous Operation

The following alerts provide information on asynchronous states between servers in a cluster or supercluster.

RealPresence Resource Manager System Integration

The following alerts provide information on RealPresence Resource Manager system integration events and changes in integration status.
Alert 2001

*<formatted string from server>*

An error occurred when the cluster responsible for RealPresence Resource Manager integration tried to synchronized data with the Polycom RealPresence Resource Manager system. The alert text describes the nature of the problem, which may require remedial action on the Polycom RealPresence Resource Manager system.

Alert 2002

*Resource management system <system-name> unreachable. Last contact on: YYYY-MM-DD HH:MM GMT+/-H[:MM].*

The cluster responsible for RealPresence Resource Manager integration was unable to connect to the Polycom RealPresence Resource Manager system.

This may indicate a network problem or a problem with the Polycom RealPresence Resource Manager system.

Try logging in to the Polycom RealPresence Resource Manager system. If you can do so, make sure the login credentials that the RealPresence DMA system uses to connect to it are still valid.

Alert 2004

*Resource management server <system-name> has inconsistent territory definitions in its site topology.*

The system is integrated with a Polycom RealPresence Resource Manager system, and there is a problem with the territory definitions or responsibility assignments in the site topology data imported from that system.

On the Polycom RealPresence Resource Manager system, configure territories properly (for instance, no duplicate names) and in way that meets the needs of the RealPresence DMA system. Assign responsibilities (primary and backup) for the territories to the appropriate RealPresence DMA clusters. A territory can only host conference rooms if it's assigned to a RealPresence DMA cluster.

**Active Directory Integration**

The following alerts provide information on changes in Active Directory integration status.

Alert 2101

*Active Directory user and group cache update was not successful on cluster <cluster>.*

The cluster responsible for Active Directory integration was unable to update the cache of user and group data.

This may indicate a network problem or a problem with the AD.

If the cluster was unable to log in to the AD server, alert 2107 is also generated.
Click the link to go to the Microsoft Active Directory page and check the Active Directory Connection section.

**Alert 2102**

*Zero enterprise conference rooms exist on cluster <cluster>.*

The cluster responsible for Active Directory integration successfully retrieved user and group data, but no conference rooms were generated.

This may indicate that no directory attribute was specified from which to generate conference room IDs, or that the chosen attribute resulted in empty (null) conference room IDs after the system removed the characters to remove.

Click the link to go to the Microsoft Active Directory page and check the Enterprise Conference Room ID Generation section. If necessary, check the Active Directory and determine an appropriate directory attribute to use.

**Alert 2104**

*Active Directory service is not available. Both primary cluster <p-cluster> and backup cluster <b-cluster> are not operational.*

The primary and backup cluster for the territory responsible for Active Directory integration are both unreachable.

This may indicate serious network problems. It is also possible that someone shut both clusters down, or shut down one and the other then failed, or both failed (unlikely).

Click the link to go to the DMAs page to begin troubleshooting. Determine whether the clusters were deliberately shut down. If not, try pinging the clusters’ IP addresses.

Other clusters can continue using the shared data store from the last cache update, so there is no immediate AD-related problem. But the unavailable clusters probably have other territory-related responsibilities (Conference Manager and/or Call Server), so you may need to assign the affected territory to some other cluster(s).

**Alert 2105**

*Active Directory service is not available. Cluster <p-cluster> is not operational.*

The primary cluster for the territory responsible for Active Directory integration is unreachable, and it has no backup cluster.

This may indicate a network problem. It is also possible that someone shut the cluster down or that it failed.

Click the link to go to the DMAs page to begin troubleshooting. Determine whether the cluster was deliberately shut down. If not, try pinging the cluster’s IP addresses.

Other clusters can continue using the shared data store from the last cache update, so there is no immediate AD-related problem. But the unavailable cluster probably has other territory-related responsibilities (Conference Manager and/or Call Server), so you may need to assign the affected territory to some other cluster.

Polycom recommends assigning a backup cluster for each territory.
Alert 2106

*Cluster* <cluster>: *Failed connection from* <server> *to Active Directory for user authentications at* YYYYY-MM-DD HH:MM GMT+/-H[/:MM].

The specified server tried to connect to the Active Directory in order to authenticate a user’s credentials and was unable to do so. This may indicate a network problem or a problem with the AD itself.

If the network and the AD itself both appear to be OK, the connection attempt may have failed because the cluster was unable to log in to the AD server.

Click the link to go to the Microsoft Active Directory page. Make sure the login credentials that the RealPresence DMA system uses to connect to Active Directory are still valid and update them if necessary.

Alert 2107

*Failed connection from* <cluster> *to Active Directory for user caching at* YYYYY-MM-DD HH:MM GMT+/-H[/:MM].

The cluster responsible for Active Directory integration was unable to log into the AD server.

Click the link to go to the Microsoft Active Directory page.

Alert 2108

*<alerting-cluster>*: *Active Directory primary cluster* <p-cluster> *associated with territory* <territory> *is not reachable. But backup cluster* <c-cluster> *is reachable.*

The territory’s primary cluster assigned to do Active Directory integration is not reachable. The territory’s backup cluster assigned to do Active Directory integration is reachable.

This may indicate a network problem. It’s also possible that someone shut the primary cluster down or that it failed.

Click the link to go to the Integrations > DMA page. Log in to the affected cluster, if possible, and check the health of the cluster. Determine whether the cluster was deliberately shut down. If not, try pinging the cluster’s IP addresses.

**Exchange Server Integration**

The following alerts provide information on changes in Exchange server integration status.

Alert 2201

*Exchange server integration primary cluster* <p-cluster> *is not operational. Integration by backup cluster* <b-cluster>.

The primary cluster for the territory responsible for Exchange server integration is unreachable, and its backup cluster has taken over responsibility for monitoring the Polycom Conferencing user mailbox and accepting or declining the meeting invitations received.

This may indicate a network problem. It’s also possible that someone shut the cluster down or that it failed.
Alerts

Click the link to go to the DMAs page to begin troubleshooting.

Alert 2202

*Exchange server integration is not available. Both primary cluster <p-cluster> and backup cluster <b-cluster> are not operational.*

The primary and backup clusters for the territory responsible for Exchange server integration are both unreachable.

This may indicate serious network problems. It is also possible that someone shut both clusters down, or shut down one and the other then failed, or both failed (unlikely).

Click the link to go to the DMAs page to begin troubleshooting. Determine whether the clusters were deliberately shut down. If not, try pinging the clusters' IP addresses.

Alert 2203

*Exchange server integration is not available. Cluster <p-cluster> is not operational.*

The primary cluster for the territory responsible for Exchange server integration is unreachable, and it has no backup cluster.

This may indicate a network problem. It's also possible that someone shut the cluster down or that it failed.

Click the link to go to the DMAs page to begin troubleshooting.

Database Status

The following alerts provide information on database events and changes in database status.

Alert 2401

*Connection to the history/audit database for cluster <cluster> has failed.*

The specified cluster is unable to communicate with its shared call history database. This may indicate a network problem, or a software failure within the cluster. The server(s) may need to be rebooted.

Go to the DMAs page to begin troubleshooting.

Alert 2402

*Connection to the configuration database for cluster <cluster> has failed.*

The specified cluster is unable to communicate with its shared configuration database. This may indicate a network problem, or a software failure within the cluster. The server(s) may need to be rebooted.

Go to the DMAs page to begin troubleshooting.
**Skype for Business Integration**

The following alerts provide information on changes in Microsoft Skype for Business integration.

**Alert 2601**

*Cluster <cluster>*: *Cannot reach Lync server <lyncserver> for presence publishing.*

The cluster cannot communicate with the specified Skype for Business server at the currently configured Next hop address. This could indicate a network problem, or a problem with the Skype for Business server.

Click the link to go to the Integrations > External SIP Peers page to begin troubleshooting. Try to ping the Skype for Business server’s Next hop address to verify basic connectivity.

**Alert 2602**

*Cluster <cluster>*: *Cannot authenticate with <lyncserver> for presence publishing.*

The cluster cannot authenticate with the specified Skype for Business server; presence will not be published for Polycom conference contacts.

This could indicate incorrect RealPresence DMA system or Skype for Business server configuration. Begin troubleshooting by verifying that the Presence Publishing settings on the Service Config > Conference Manager Settings > Conference Settings page are correct.

Click the link to go to the Integrations > External SIP Peers page.

**Alert 2603**

*Cluster <cluster>*: *Invalid Lync account URI configured for Lync server <lyncserver>.*

The system is unable to authenticate with the Skype for Business server using the currently configured Skype for Business account URI.

Click the link to go to the Integrations > External SIP Peers page to begin troubleshooting. Try reentering the Skype account URI for the Skype for Business server on the Skype Integration tab.

**Alert 2604**

*Cluster <cluster>*: *Cannot reach Lync server <lyncserver> to resolve conference IDs for RealConnect™ conferences.*

The system is unable to connect to the specified Skype for Business server at the currently configured Next hop address. Attempts to connect to a Skype for Business conference through the RealPresence DMA system will fail.

This could indicate a network problem, or that someone has shut down the Skype for Business server.

Click the link to go to the Integrations > External SIP Peers page to begin troubleshooting. Try pinging the specified Skype for Business server’s IP address. If it is reachable, verify that the Next hop address, Port, and Transport type settings on this page are correct.
Alert 2605

_Cluster <cluster>: Cannot authenticate with <lyncserver> to resolve conference IDs for RealConnect™ conferences._

The system cannot authenticate with the specified Skype for Business server, preventing RealConnect™ conference ID resolution. Attempts to connect to RealConnect™ conferences through the RealPresence DMA system will fail.

Click the link to go to the Integrations > External SIP Peers page to begin troubleshooting. Verify that the Transport Type is set to TLS, and that the Skype account URI on the Skype Integration tab is correct. If the RealPresence DMA system configuration is correct, investigate the Skype for Business server’s configuration.

_Signaling_

The following alerts provide information on signaling events and changes in signaling status.

Alert 3001

_No signaling interface enabled for cluster <cluster>. SIP, H.323, or WebRTC must be configured to allow calls._

The specified cluster does not have signaling enabled and is unable to accept calls.

To use the cluster for anything other than logging into the management interface, you must enable signaling.

If you are logged in to that cluster, click the link to go to the Signaling Settings page. If not, log into that cluster and go to Admin > Server > Signaling Settings.

_Certificate_

The following alerts provide information on changes in certificate status such as certificate expirations and incompatibilities.

Alert 3101

_Cluster <cluster>: The server certificate has expired._

The specified cluster’s server certificate has expired. This is the public certificate that the cluster uses to identify itself to devices configured for secure communication. The cluster can no longer communicate with any such devices, including MCUs, endpoints, the AD server, and the Exchange server.

If you are logged in to that cluster, click the link to go to the Certificates page. If not, log in to that cluster (your browser will warn you not to do this, and you will have to override its advice) and go to Admin > Server > Certificates.
Alert 3102

*Cluster <cluster>*: The server certificate will expire within 1 day. All system access may be lost.

The specified cluster’s server certificate is about to expire. This is the public certificate that the cluster uses to identify itself to devices configured for secure communication. If you allow it to expire, the cluster will no longer be able to communicate with any such devices, including MCUs, endpoints, the AD server, and the Exchange server.

If you are logged in to that cluster, click the link to go to the Certificates page. If not, log in to that cluster and go to Admin > Server > Certificates.

Alert 3103

*Cluster <cluster>*: The server certificate will expire within <count> days. All system access may be lost.

The specified cluster’s server certificate will soon expire. This is the public certificate that the cluster uses to identify itself to devices configured for secure communication. If you allow it to expire, the cluster will no longer be able to communicate with any such devices, including MCUs, endpoints, the AD server, and the Exchange server.

If you are logged in to that cluster, click the link to go to the Certificates page. If not, log in to that cluster and go to Admin > Server > Certificates.

Alert 3104

*Cluster <cluster>*: One or more CA certificates have expired.

The specified cluster has an expired CA certificate or certificates. When a CA certificate expires, the certificates signed by that certificate authority are no longer accepted. Depending on its security settings, the cluster may refuse connections from devices presenting a certificate signed by a CA whose certificate has expired, including MCUs, endpoints, the AD server, and the Exchange server.

If you are logged in to that cluster, click the link to go to the Certificates page. If not, log in to that cluster and go to Admin > Server > Certificates.

If that cluster has Skip validation of certificates for inbound connections turned off, you will not be able to log into it. Contact Polycom Global Services.

Alert 3105

*Cluster <cluster>*: One or more CA certificates will expire within 30 days.

The specified cluster has a CA certificate or certificates that will expire soon. When a CA certificate expires, the certificates signed by that certificate authority are no longer accepted. If you allow the CA certificate(s) to expire, depending on its security settings, the cluster may refuse connections from any devices presenting a certificate signed by a CA whose certificate has expired, including MCUs, endpoints, the AD server, and the Exchange server.

If you are logged in to that cluster, click the link to go to the Certificates page. If not, log in to that cluster and go to Admin > Server > Certificates.
Alert 3108

**Cluster <cluster>: The server SSL certificate is incompatible with the cluster's network settings.**

The specified server’s SSL certificate does not match the cluster’s domain information or other network configuration. Perhaps the network configuration was changed, and the SSL certificate is now out of date.

If you are logged in to that cluster, click the link to go to the **Certificates** page. If not, log in to that cluster and go to **Admin > Server > Certificates**. Try regenerating the SSL certificate in question.

**Licenses**

The following alerts provide information on changes in licensing status.

Alert 3201

**Cluster <DMA URL> has no license. Either apply license key(s) or configure Clariti licenses through the Polycom Licensing Center. System will allow up to 10 concurrent calls.**

You have not entered the license key(s) for the specified cluster.

If you are logged in to that cluster, click the link to go to the **Licenses** page. If not, log in to that cluster and go to **Admin > Server > Licenses**.

Without a valid license, the cluster is limited to ten simultaneous calls.

Alert 3202

**Invalid license key(s) applied to cluster <cluster>. System will allow up to 10 concurrent calls.**

The specified cluster has an invalid license key or keys.

If you are logged in to that cluster, click the link to go to the **Licenses** page. If not, log in to that cluster and go to **Admin > Server > Licenses**.

Without a valid license, the cluster is limited to ten simultaneous calls.

Alert 3203

**The EULA for cluster <cluster> has not been accepted. All calls are blocked on this cluster.**

The system version has changed, and the End User License Agreement has not yet been accepted. The specified cluster will not accept any inbound calls or place outbound calls, until a user with Administrator privileges accepts the agreement upon login.

Click the link to go to the **Licenses** page, where you can view the EULA acceptance status and details.
Alert 3204

**Cluster <cluster>: Cannot connect to licensing server <lserver>**.

The specified cluster cannot connect to the licensing server, or there is no licensing server configured for this cluster.

If you are logged in to that cluster, click the link to go to the **Licenses** page to view licensing details. Check the status of licensing by logging in to the RealPresence Platform Director system.

Alert 3205

**Cluster <cluster>: DMA VE Soft RPP version is incompatible with license. No calls are permitted.**

The specified cluster’s version of software is not compatible with the installed license. The system will not permit calls until a license that has been activated for this version of software is installed.

Click the link to go to the **Licenses** page to install the proper license activation key.

Alert 3206

**Cluster <cluster>: DMA is not licensed for any calls.**

The current license for the specified cluster does not include the ability to make calls.

Click the link to go to the **Licenses** page to view licensing details or install a different license activation key.

**Networks**

The following alerts provide information on network errors and connectivity.

Alert 3301

**Cluster <cluster> is configured for 2 servers, but only a single server is detected.**

One of the servers in the specified cluster is not responding to the other server over the private network that connects them.

This could be a hardware problem, or the server in question may just need to be rebooted. It is also possible that the private network connection between the two servers has failed. Check the Ethernet cable connecting the GB 2 ports (Polycom Rack Server 630 or 620-based systems) or the Port 1 ports (Polycom Rack Server 220-based systems) and replace it if necessary.

Alert 3302

**Cluster <cluster> is configured for 1 server, but the private network interface is enabled and active.**

Either the cluster contains two servers but was incorrectly configured as a single-server cluster, or there is only one server in the cluster but something is connected its GB 2 port (Polycom Rack Server 630 or 620-based systems) or Port 1 port (Polycom Rack Server 220-based systems).
On a single-server cluster, do not use the server’s GB 2 port (Polycom Rack Server 630 or 620-based systems) or Port 1 port (Polycom Rack Server 220-based systems) for anything.

**Alert 3303**

.Cluster <cluster>: A private network error exists on <server>. The specified server has detected a problem with the private network that connects the two servers in the cluster.

For systems installed on a Polycom Rack Server 630 (R630) or 620 (R620), this could be a problem with the GB 2 Ethernet port (eth1 interface). For systems installed on a Polycom Rack Server 220 (R220), this could be a problem with the Port 1 Ethernet port (eth1 interface).

This could also be a problem with the Ethernet cable connecting the eth1 interfaces of the two systems. Or, the server in question may just need to be rebooted.

**Alert 3304**

.Cluster <cluster>: A public network error exists on <server>. The specified server has detected a problem with the management (or combined management and signaling) network connection.

For systems installed on a Polycom Rack Server 630 (R630) or 620 (R620), this could be a problem with the GB 1 Ethernet port (eth0 interface). For systems installed on a Polycom Rack Server 220 (R220), this could be a problem with the Port 0 Ethernet port (eth0 interface).

This could also be a problem with the Ethernet cable connecting the server to the enterprise network switch, or that switch.

Or, the server in question may just need to be rebooted.

**Alert 3305**

.Cluster <cluster>: A signaling network error exists on <server>. The specified server has detected a problem with the signaling network connection.

For systems installed on a Polycom Rack Server 630 (R630) or 620 (R620), this could be a problem with the GB 3 port (eth2 interface). For systems installed on a Polycom Rack Server 220 (R220), this could be a problem with the GB 1 port (eth2 interface).

This could also be a problem with the Ethernet cable connecting the server to the enterprise network switch, or that switch. Or, the server in question may just need to be rebooted.

**Alert 3306**

.DNS <address of DNS server> settings are inconsistent with network configuration on Cluster <cluster>: <issue-text>. The system has found issues with the DNS configuration on the Admin > Server > Network Settings page for the specified cluster. This could indicate one of the following possible problems:
The virtual or management host name A or AAAA record configured in the specified DNS server is missing

The virtual or management host name A or AAAA record configured in the specified DNS server references the incorrect address

The alert text describes the nature of the problem, which may require additional configuration of the DNS server(s) or network settings for the cluster.

Refer to the Polycom RealPresence DMA System Operations Guide for more information regarding DNS configuration.

Click the link to go to the Admin > Server > Network Settings page.

**Alert 3309**

*Cluster <cluster>: DNS <address of DNS server> is unresponsive. <service> at <FQDN> <referenced by> {will use <IP address> | cannot be reached}.*

One or more configured DNS servers are not responding to requests from the specified cluster. The system will use the last cached IP address for the DNS server, but if no IP address is known, this DNS server is considered unreachable.

This could indicate a network problem, or that a DNS server is out of service.

Click the link to go to the Admin > Server > Network Settings page.

**Alert 3310**

*Cluster <cluster>: DNS <address of server> cannot resolve <FQDN>. <service> <referenced by> cannot be reached.*

The specified cluster cannot resolve the domain name of this Active Directory, MCU, ISDN gateway, or DMA cluster. The specified service is currently unreachable.

This could indicate a network problem, or that the specified domain name entry is incorrect in the DMA cluster’s configuration.

If the alert originated from a different cluster, log in to that cluster and go to the Admin > Server > Network Settings page to begin troubleshooting. If you are already logged in to the originating cluster, click the link to go to the Admin > Server > Network Settings page.

**Server Resources**

The following alerts provide information on changes in the resources of the server or cluster.

**Alert 3401**

*Cluster <cluster>: Available disk space is less than 15% on server <server>.*

The specified cluster is running out of disk space.

Suggestions for recovering and conserving disk space include:

- Delete backup files (after downloading them).
● Remove upgrade packages.
● History data is written to the backup file nightly. Reduce history retention settings so the same history data is not being repeatedly backed up.
● Roll logs more often (compressing the data) and make sure Logging level is set to Production.

**Alert 3403**

*Cluster <cluster>: Log files on server <server> exceed the capacity limit and will be purged within 24 hours.*

Log archives on the specified cluster exceed the capacity limit for logs. After midnight, the system will delete sufficient log archives to get below the limit.

Click the link to go to the System Log Files page. We recommend routinely downloading archived logs and then deleting them from the system.

**Alert 3404**

*Cluster <cluster>: Log files on server <server> are close to capacity and may be purged within 24 hours.*

Log archives on the specified cluster have reached the percentage of capacity that triggers an alert, set on the Alerting Settings page.

Click the link to go to the System Log Files page. We recommend routinely downloading archived logs and then deleting them from the system.

**Alert 3405**

*Server <server> CPU utilization >50% and <75%.*

The specified server’s CPU and/or I/O bandwidth usage is unusually high.

This can be caused by activities such as backup creation, CDR downloading, logging at too high a level, or refreshing an extremely large Active Directory cache.

The cause may also be a system health problem or a runaway process. Go to Admin > Troubleshooting Utilities > Top to see if a process is monopolizing CPU resources.

Create a new backup and download it, and then contact Polycom Global Services.

**Alert 3406**

*Server <server> CPU utilization > 75%.*

The specified server’s CPU and/or I/O bandwidth usage is exceptionally high.

This can be caused by activities such as backup creation, CDR downloading, logging at too high a level, or refreshing an extremely large Active Directory cache.

The cause may also be a system health problem or a runaway process. Go to Admin > Troubleshooting Utilities > Top to see if a process is monopolizing CPU resources.

Create a new backup and download it, and then contact Polycom Global Services.
Data Synchronization

The following alerts provide information on changes in data synchronization between servers in the cluster.

Alert 3601

Cluster <cluster>: System version differs between servers.

The specified cluster is supposed to have two servers, but a software version mismatch makes it impossible for them to form a redundant two-server cluster.

Possible explanations:

- Someone upgraded one server of the cluster while the other was turned off or otherwise unavailable.
- An expansion server was added to a single-server cluster, but the new server was not patched to the same software level as the existing server.
- An RMA replacement server was not patched to the same software level as the existing server.

If you are logged in to that cluster, click the link to go to the Software Upgrade page. If not, log in to that cluster and go to Admin > Software Upgrade. Check Operation History.

Log into the physical address of the server that was unable to join the cluster and upgrade it to match the other server. After it restarts, it will join the cluster.

Alert 3602

Cluster <cluster>: Local time differs by more than ten seconds between servers.

The time on the two servers in the specified cluster has drifted apart by an unusually large amount. This may indicate a configuration issue or a problem with one of the servers. Contact Polycom Global Services.

Alert 3603

Cluster <cluster>: Active Directory integration is not consistent between servers.

In the specified cluster, the Active Directory integration status information is different on the two servers, indicating that their internal databases are not consistent.

Try to determine which server's data is incorrect and reboot it.

Alert 3604

Cluster <cluster>: Enterprise conference rooms differ between servers.

In the specified cluster, the enterprise conference room counts are different on the two servers, indicating that their internal databases are not consistent.

Try to determine which server's data is incorrect and reboot it.
Alert 3605

*Cluster <cluster>*: *Custom conference rooms differ between servers.*

In the specified cluster, the custom conference room counts are different on the two servers, indicating that their internal databases are not consistent.

Try to determine which server’s data is incorrect and reboot it.

Alert 3606

*Cluster <cluster>*: *Local users differ between servers.*

In the specified cluster, the local users are different on the two servers, indicating that their internal databases are not consistent.

Try to determine which server’s data is incorrect and reboot it.

**System Health and Availability**

The following alerts provide information on changes in the health and availability of the system.

Alert 3801

<d-cluster>: Cluster <f-cluster>/server <f-server> failover to <b-server> due to <component> failure: <details of failure>

The cluster from which the alert originated is reporting that a server in a different cluster has failed over to an alternate server because of an internal software component failure. The alert includes details on what component experienced the failure.

This alert is cleared when the condition that caused the alert is resolved.

Use the failure details as a starting point for troubleshooting. If the failure is not hardware or network related, and you are unable to access the server, it may need to be rebooted.

Click the link to go to the **Integrations > DMA** page.

Alert 3802

<d-cluster>: Cluster <f-cluster>/server <f-server> restarted due to <component> failure: <details of failure>

The cluster from which the alert originated is reporting that a server in a different cluster has restarted because of an internal component failure. The alert includes details on what component experienced the failure.

Use the failure details as a starting point for troubleshooting. If the failure is not hardware or network related, and you are unable to access the server, it may need to be physically powered off and powered back on.

Click the link to go to the **Integrations > DMA** page.
Alert 3803

<d-cluster>: Cluster <f-cluster>/server <f-server> is operating in an impaired state due to <component> issue: <details of impairment>

The cluster from which the alert originated is reporting that a server in a different cluster has experienced one or more software component issues, and is running in an unhealthy state. The alert includes further details of the impairment of the system.

Use the impairment details as a starting point for troubleshooting. If the impairment is not hardware or network related, and you are unable to access the server, it may need to be rebooted.

Click the link to go to the Integrations > DMA page.

Cluster Features

The following alerts provide information on the status of certain cluster operations.

Alert 3901

<cluster>: Scheduled backup at <date-time> failed because the remote server address could not be resolved.

The specified cluster could not resolve the hostname or IP address of the remote backup server, causing the backup scheduled at <date-time> to fail.

This alert is cleared the next time a scheduled backup is successful, regardless of any configuration changes.

Click the link to go to the Admin > Server > Backup Settings page. Ensure the hostname or IP address for the remote backup server is correct, and that the server is reachable from the RealPresence DMA system.

Alert 3902

<cluster>: Scheduled backup at <date-time> failed because there was no response from the remote server.

The specified cluster did not receive a response from the configured remote backup server, causing the backup scheduled at <date-time> to fail.

This alert is cleared the next time a scheduled backup is successful, regardless of any configuration changes.

Click the link to go to the Admin > Server > Backup Settings page.

Alert 3903

<cluster>: Scheduled backup at <date-time> failed because the configured login/password for the remote server are invalid.

The specified cluster was unable to authenticate with the configured remote backup server using the configured login and password, causing the backup scheduled at <date-time> to fail.
This alert is cleared the next time a scheduled backup is successful, regardless of any configuration changes.

Click the link to go to the Admin > Server > Backup Settings page. Ensure the credentials for the remote backup server are correct.

Alert 3904

<cluster>: Scheduled backup at <date-time> failed because there was a data transfer error with the remote server.

A communications error with the backup server caused the backup scheduled at <date-time> to fail.

This alert is cleared the next time a scheduled backup is successful, regardless of any configuration changes.

Click the link to go to the Admin > Server > Backup Settings page. Ensure the network link between the RealPresence DMA system and the remote backup server is reliable.

Alert 3905

<cluster>: Scheduled backup at <date-time> failed because the backup file could not be created.

The RealPresence DMA system was unable to create the backup file on the remote backup server, causing the backup scheduled at <date-time> to fail.

This alert is cleared the next time a scheduled backup is successful, regardless of any configuration changes.

Click the link to go to the Admin > Server > Backup Settings page. Check the remote backup server’s file system permissions to ensure the RealPresence DMA system can create and write to files there.

MCUs

The following alerts provide information on changes in the status of connected MCUs.

Alert 4001

MCU <MCUname> is currently busied out.

Someone busied out the specified MCU.

Click the link to go to the Integrations > MCU page.

Alert 4002

MCU <MCUname> is currently out of service.

Someone took the specified MCU out of service.

Click the link to go to the Integrations > MCU page.
Alert 4003

MCU <MCUname> has <count> warning(s).

The MCUs page is displaying warnings related to the specified MCU.
Click the link to go to the Integrations > MCU page for more information.

Alert 4004

MCU <MCUname> is configured with insufficient user connections.

The system was unable to establish an additional management session connection to the specified MCU.
Possible explanations:
- IP connectivity between the system and the MCU has been lost.
- This MCU does not allow sufficient connections per user.

Polycom MCUs use synchronous communications. In order to efficiently manage multiple calls as quickly as possible, the Polycom RealPresence DMA system uses multiple connections per MCU. By default, a RealPresence Collaboration Server or RMX MCU allows up to 20 connections per user (the MAX_NUMBER_OF_MANAGEMENT_SESSIONS_PER_USER system flag). We recommend not reducing this setting. If you have a RealPresence DMA supercluster with three Conference Manager clusters and a busy conferencing environment, we recommend increasing this value to 30.

After a connection attempt fails and this alert is triggered, the system tries every 60 seconds to establish 5 connections to this MCU. If it succeeds, this alert is automatically cleared.
Click the link to go to the Integrations > MCU page.

Alert 4005

MCU <MCUname> is disconnected.

The reporting cluster is unable to connect to the specified MCU.
This may indicate a network problem. It is also possible that someone shut the MCU down or that it failed.
Click the link to go to the Integrations > MCU page for more information.

Alert 4009

MCU <mcu> disconnect rate is > 1 and < 4.

The RealPresence DMA cluster has lost connection with the specified MCU between one and four times in the past 24 hours.
This most likely indicates a network problem, but it could also indicate that the MCU or RealPresence DMA system is under very heavy load. If the MCU stays connected for more than 24 hours, this alert is cleared, but if the RealPresence DMA system loses connection with this MCU more than 4 times in 24 hours, this alert is replaced with Alert 4010.
Click the link to go to the Integrations > MCU page to begin troubleshooting. Check the network connection between this MCU and the RealPresence DMA cluster.
Alert 4010

**MCU <mcu> disconnect rate is > 4.**

The DMA cluster has lost connection with the specified MCU more than four times in the past 24 hours. This most likely indicates a network problem, but it could also indicate that the MCU or RealPresence DMA system is under very heavy load.

Click the link to go to the Integrations > MCU page to begin troubleshooting. Check the network connection between this MCU and the RealPresence DMA cluster.

Alert 4011

**MCU <mcu> call failure penalty is > 0.4 and < 0.8.**

The specified MCU’s number of consecutive failed calls has changed, and the calculated failure penalty metric is now between 0.4 (some calls are failing) and 0.8 (most calls are failing).

The RealPresence DMA system keeps track of per-MCU call failure penalties not only to alert administrators to call failures, but also to ensure that calls will be routed less often to MCUs with high call failure penalties.

Click the link to go to the Integrations > MCU page to begin troubleshooting.

Alert Availability and Reliability Tracking

Alert 4012

**MCU <mcu> call failure penalty is > 0.8.**

The specified MCU’s number of consecutive failed calls has changed, and the calculated failure penalty metric is now above 0.8.

This indicates that most of the specified MCU’s calls are failing. The RealPresence DMA system keeps track of per-MCU call failure penalties not only to alert administrators to call failures, but also to ensure that calls will be routed less often to MCUs with high call failure penalties.

Click the link to go to the Integrations > MCU page to begin troubleshooting.

Alert Availability and Reliability Tracking

Alert 4013

**MCU <mcu> is connected with no port capacity.**

The specified MCU has no ports available for call traffic.

This could indicate that the specified MCU is at capacity, or possibly a network problem. This alert appears as soon as the port capacity of this MCU becomes 0, and is automatically cleared after two minutes.

Click the link to go to the Integrations > MCU page to begin troubleshooting.
Alert 4014

**MCU <mcu> video port capacity changed from <oldcapacity> to <newcapacity>.**

The video port capacity of the specified MCU has changed.

This could indicate a license change, video / voice port configuration change, or hardware change for the MCU (perhaps a media card has been removed or added). This alert appears as soon as the video port capacity of this MCU becomes 0, and is automatically cleared after two minutes.

Click the link to go to the Integrations > MCU page.

Alert 4015

**MCU <mcu> voice port capacity changed from <oldcapacity> to <newcapacity>.**

The voice port capacity of the specified MCU has changed.

This could indicate a license change, video / voice port configuration change, or hardware change for the MCU (perhaps a media card has been added or removed). This alert appears as soon as the voice port capacity of this MCU becomes 0, and is automatically cleared after two minutes.

Click the link to go to the Integrations > MCU page.

Alert 4016

**MCU <mcu> has been automatically busied out due to <N> consecutive failures to start conferences. Investigate the MCU state and logs.**

The specified MCU has been automatically busied out because it failed to start <N> number of conferences in a row. This condition is likely caused by an MCU software issue. Non-consecutive failures to start calls do not trigger this condition.

Once the MCU is busied out, when the last conference ends on the MCU, the MCU automatically changes to the Out of Service state. Once that happens, this alert is replaced with Alert 4017.

Click the link to go to the Integrations > MCU page.

Alert 4017

**MCU <mcu> has been automatically placed out of service due to <N> consecutive failures to start conferences. Investigate the MCU state and logs.**

The specified MCU has been placed in the Out of Service state after it was automatically busied out because it failed to start <N> number of conferences in a row. This condition is likely caused by an MCU software issue.

This alert replaces Alert 4016.

Click the link to go to the Integrations > MCU page.
Alert 4018

**MCU <mcu> MCCF connection limit exceeded. Some conference features will not work.**

The MCCF (Media Control Channel Framework) connection limit for the specified MCU has been exceeded, because there are too many RealPresence DMA systems connecting to this MCU.

Additional RealPresence DMA systems will connect to this MCU without MCCF, but some IVR, VEQ, passcode, and CDR features will not work correctly.

To correct this problem, reduce the number of RealPresence DMA systems simultaneously connecting to this MCU.

Click the link to go to the **Network < MCU > MCUs** page.

Endpoints

The following alerts provide information on communication issues with endpoints.

Alert 5001

**<Model> ITP system attempting to register with ID <H.323 ID or SIP URI> is improperly configured.**

A device that identifies itself as an ITP (Immersive Telepresence) system has registered with the Call Server, but the H.323 ID or SIP URI of the device doesn't specify its endpoint number or the number of endpoints in the ITP system, as it should.

The H.323 ID or SIP URI must be updated on the endpoints of the ITP system.

[Naming ITP Systems for Recognition by the Polycom RealPresence DMA System](#)

Alert 5002

**One or more endpoints are sending too much <signaling_type> signaling traffic. They have been temporarily blacklisted and may have been quarantined.**

At least one device, in violation of protocol standards, is sending too much of the specified type of signaling traffic (H.323 or SIP) to the RealPresence DMA system.

If there are many such ill-behaved devices, it could affect the RealPresence DMA system's ability to provide service, so the system temporarily blacklists any such device (ignoring all signaling from it until it stops sending messages more frequently than the specification permits). Depending on the registration policy, it could also be quarantined, and it remains so until manually removed from quarantine.

Click the link to go to the **Network > Endpoints** page, where you can search for endpoints with **Registration status** of Quarantined or Quarantined (Inactive).
Alert 5003

*The* `<device model>` *device identified by* `[<device identifier>]` *is no longer registered to the call server.*

The specified device has unregistered or its registration has expired. This alert appears only if it has been enabled for this endpoint or MCU. This alert is automatically cleared after two minutes.

Click the link to go to the Endpoints page.

Alert 5004

`<sigtype>` call from `<originator>` to `<dial string>` was dropped due to routing loop.

As the system tried to route the H.323 or SIP call from its source to the destination, a dialing loop in the site topology was detected, and the call was dropped.

Click the link to go to the Reports > Call History page and view more information about the call. See Suggestions for Modifying the Default Dial Plan for common ways to avoid dialing loops.

Conference Manager

The following alerts provide information on possible problems with conference manager functionality.

Alert 6001

**No territories configured to host conference rooms.**

You must enable a territory to host conference rooms in order to use the cluster responsible for the territory as a Conference Manager. You can enable up to three territories to host conference rooms.

Click the link to go to the Service Config > Site Topology > Territories page.

Alert 6002

*Shared number dialing VEQ* `<VEQnum>` *references entry queue* `<EQname>` *which is not configured on any MCUs.*

The specified entry queue used by the VEQ `<VEQnum>` is not configured on an MCU. If the VEQ is a Direct Dial VEQ, `<VEQnum>` is “Direct Dial”.

Click the link to go to Service Config > Conference Manager Settings > Shared Number Dialing to begin troubleshooting. Ensure that at least one MCU configured in Integrations > MCU has the specified entry queue configured.

Shared Number Dialing

Conference Status

The following alerts provide information on some types of call failures.
Alert 6101

**Call failed: Preset dialout from conference VMR <VMR> to <destination> failed.**
**Cause: <cause>**

A preset dialout from the conference using the conference room identifier <VMR> has failed for the specified reason. This alert automatically clears after two minutes.

Click the link to go to the Network > Users page to find the specified VMR number and begin troubleshooting.

Alert 6102

**Conference <VMR> on MCU <MCU> failed to start: <reason>.**

A conference using the conference room identifier <VMR> has failed to start for the specified reason. If no MCU was selected, <MCU> is “unresolved”. This alert automatically clears after two minutes.

Click the link to go to the Network > Users page to find the specified VMR number and begin troubleshooting.

Alert 6103

**Ongoing conference <VMR> on MCU <MCU> failed: <reason>.**

A conference using the conference room identifier <VMR> has been aborted for the specified reason. This alert automatically clears after two minutes.

Click the link to go to the Network > Users page to find the specified VMR number and begin troubleshooting.

Alert 6104

**Ongoing conference <VMR> on MCU <MCU1> failed over to MCU <MCU2>: <reason>.**

A conference using the conference room identifier <VMR> has been moved from <MCU1> to <MCU2> for the specified reason. This alert automatically clears after two minutes.

Click the link to go to the Network > Users page to find the specified VMR number and begin troubleshooting.

Alert 6105

**Integrations > Microsoft Active Directory > Lync RealConnect™ Callback contacts OU value, ‘<OU>’, does not exist in Active Directory.**

The system is unable to find the specified OU in Active Directory, and will be unable to start RealConnect™ conferences using external Lync systems.

When you integrate with an external Lync system, the RealPresence DMA system uses an Active Directory contact from the OU specified in this field to receive calls forwarded from the external Lync system.
Alerts

Click the link to go to the Integrations > Microsoft Active Directory page. Verify that the value for the Callback contacts OU field is correct and contains valid contacts that the system can use for this purpose.

Alert 6106

RealConnect\textsuperscript{TM} conference with external Lync system cannot start. There are no available callback contacts.

The system is unable to find any callback contacts to use in the OU specified on the Integrations > Microsoft Active Directory page. RealConnect\textsuperscript{TM} conferences with external Skype for Business systems will not start.

When you integrate with an external Skype for Business system, the RealPresence DMA system uses an Active Directory contact from the OU specified on this page to receive calls forwarded from the external Skype for Business system.

Click the link to go to the Integrations > Microsoft Active Directory page. Verify that the value for the Callback contacts OU field is correct and contains valid contacts that the system can use for this purpose.

Alert 6107

Conference factory - all generated dynamic conference IDs are in use.

The system is unable to create a conference because the maximum number of dynamic conference IDs have been generated.

Alert 6108

Conference factory - too many conference factory requests received.

The system is unable to create a conference because protection against Denial of Service (DOS) attacks has been activated.

Skype for Business Presence Publishing

The following alerts provide information on problems the system may encounter when publishing presence for Polycom conference contacts.

Alert 6201

Cluster <cluster>: Errors in presence publication for Lync server <lyncserver>. Presence for <NN> of <MM> Polycom conference contacts will not be published due to Lync server configuration ‘MaxEndpointExpiration’ value <expire>.

The system was unable to publish presence status for the specified number of Polycom conference contacts because the Skype for Business server has been configured with a maximum endpoint logon period of <expire> seconds.

To publish presence status for Polycom conference contacts, the RealPresence DMA system registers each contact with the Skype for Business server every ‘MaxEndpointExpiration’ seconds. Depending on how many conference contacts are configured for presence publishing, the RealPresence DMA system may be
unable to publish presence for all contacts during this interval, as the system registers one conference contact per second.

If suitable for your environment, either increase the ‘MaxEndpointExpiration’ value on the Skype for Business server, or decrease the number of Polycom conference contacts configured for publishing.

Click the link to go to the Integrations > External SIP Peers page.

**Alert 6202**

*Cluster <cluster>: Errors in presence publication for Lync server <lyncserver>.*
*Presence for <NN> of <MM> Polycom conference contacts will not be published because the number of Polycom conference contacts configured for publishing exceeds ‘Maximum Polycom conference contacts to publish’ configured on the system.*

The system was unable to publish presence status for the specified number of Polycom conference contacts because the Maximum Polycom conference contacts to publish value configured in the Skype for Business server’s External SIP Peer properties has been reached.

Click the link to go to the Integrations > External SIP Peers page to begin troubleshooting. If suitable for your environment, increase the Maximum Polycom conference contacts to publish value.

**Alert 6203**

*Cluster <cluster>: Errors in presence publication for Lync server <lyncserver>.*
*Presence for <NN> of <MM> Polycom conference contacts will not be published: the system is unable to complete publication within the expiration interval.*

The system was unable to publish presence status for the specified number of Polycom conference contacts within the number of seconds specified by the ‘MaxEndpointExpiration’ setting on the Skype for Business server.

To publish presence status for Polycom conference contacts, the RealPresence DMA system registers each contact with the Skype for Business server every ‘MaxEndpointExpiration’ seconds. This alert could indicate heavy RealPresence DMA system load or other performance-related factors during presence publishing.

If suitable for your environment, either increase the ‘MaxEndpointExpiration’ value on the Skype for Business server, or decrease the number of Polycom conference contacts configured for publishing.

Click the link to go to the Integrations > External SIP Peers page.

**Alert 6205**

*Cluster <cluster>: Failed to create/manage conference contacts in Active Directory; DMA time is skewed from Active Directory’s time.*

The specified cluster has attempted to create or manage Active Directory conference contacts, and failed because the system time differs between the RealPresence DMA system and the Active Directory system.

If possible, ensure that the RealPresence DMA system and your Active Directory system both use the same NTP server.
Alerts

Click the link to go to the **Integrations > Microsoft Active Directory** page.

**Alert 6206**

*Cluster <cluster>: Failed to create/manage conference contacts in Active Directory; DNS cannot resolve the “<setting>”, <FQDN>, configured at <page>.*

The specified cluster has attempted to create or manage Active Directory conference contacts, and failed. The cluster either cannot resolve the IP address or host name configured on the **Integrations > Microsoft Active Directory** page, or the Next hop address configured for the specified SIP peer on the **Integrations > External SIP Peers** page.

Go to the page specified in the alert, and verify that the configuration is correct. If so, verify your network’s DNS configuration.

Click the link to go to the page specified in the alert.

**Alert 6207**

*Cluster <cluster>: Failed to create/manage conference contacts in Active Directory; invalid domain, user name, or password.*

The specified cluster has attempted to create or manage Active Directory conference contacts, and failed because the domain, user name, or password is incorrect on the **Integrations > Microsoft Active Directory** page.

Click the link to go to the **Integrations > Microsoft Active Directory** page, and verify that the Domain, Domain/user name, and Password fields are correct.

**Alert 6208**

*Cluster <cluster>: Failed to create/manage conference contacts in Active Directory; Active Directory is not configured for Windows Remote Management.*

The specified cluster has attempted to create or manage Active Directory conference contacts, and failed because the Active Directory system is not configured for Windows Remote Management.

For details on enabling Windows Remote Management on your Active Directory system, refer to the *Polycom Unified Communications for Microsoft Environments - Solution Deployment Guide*.

Click the link to go to the **Integrations > Microsoft Active Directory** page.

**Alert 6209**

*Cluster <cluster>: Failed to create/manage conference contacts in Active Directory; Active Directory reports error: <text>.*

The specified cluster has attempted to create or manage Active Directory conference contacts, and failed. The Active Directory system has reported <text> in response to the RealPresence DMA system’s request. Use the error text to begin troubleshooting.

Click the link to go to the **Integrations > Microsoft Active Directory** page.
Call Server

The following alerts provide information on issues with call server functionality.

Alert 7001

*Failed registration data incomplete: cluster *<cluster>* history limited to *<n.n>* hours.*

Registration data retention settings are too low for the system to determine the number of failed registrations in the past 24 hours.

Click the link to go to the Admin > Server > History Retention Settings page and increase the number of registration records to retain on each cluster.

Alert 7005

*Site *<sitename>* has no available aliases for automatic ISDN assignment.*

The specified site is configured for automatic E.164 alias number assignment, but all of the aliases within the specified range are already assigned.

Click the link to go to the Service Config > Site Topology > Sites page to begin troubleshooting. Try expanding the ISDN number ranges specified in the site's ISDN Range Assignment section.

Alert 7006

*Cluster *<cluster>*: External SIP peer *<sippeer>* is unresponsive.*

The specified cluster has detected that the external SIP peer named *<sippeer>* is not responding.

Click the link to go to the Integrations > External SIP Peers page to view the settings of the specified external SIP peer.

Call Bandwidth Management

The following alerts provide information on possible bandwidth management issues and other bandwidth management events.

Alert 7101

*<N> Calls rejected starting at *<time>* due to lack of bandwidth on *<throttlepoint-type>* *<throttlepoint>*.*

The DMA system has disallowed the specified number of calls *<N>* from starting, as there is not enough bandwidth to carry the calls on the site topology segment (subnet, site, or site link) with the name *<throttlepoint>*.

Click the link to go to the Reports > Call History page, where the first call to be rejected during this event is displayed. If possible in your environment, increase the bandwidth available to this subnet, site, or site link.
Troubleshooting Utilities

The Polycom® RealPresence® DMA® system includes various network and system troubleshooting utilities.

- Run Network Packet Capture
- Run Ping
- Run Traceroute
- Run Top
- Run I/O Stats
- Run SAR
- Manually Synchronize all Clusters
- Check NTP Status
- Reset to Default Settings
- Diagnostics for your Polycom Server

Run Network Packet Capture

Run Network Traffic Capture to capture data packets received or sent by the network interfaces on your RealPresence DMA system. The traffic capture generates a packet capture (.pcap) file that contains the network traffic information.

If needed, you can apply a filter on the network interface for which you capture packets. Conditional statements determine which data is captured. For example, a filter might capture data coming from ABC route and having W.X.Y.Z IP address. Example filters include the following:

- host src, dst
- tcp, udp, icmp
- src port 1025 and tcp
- portrange 21-23
- src 10.0.1.1 and port 80
- src 10.0.2.1 and (dst port 3389 or 22)
- dst host 192.168.1.1 and (dst port 80 or dst port 443)

For a description of pcap filters see http://www.tcpdump.org/manpages/pcap-filter.7.html.

To run Network Traffic Capture and download a .pcap file:

1. Go to Admin > Troubleshooting Utilities > Network Packet Capture.
2. Enter a Pcap filter or accept the default to Capture all packets.
3. Select the **Capture Interfaces** for which to capture packets.

4. Click **Capture** to start the packet capture.

5. Click **Stop** to stop the capture.
   - The RealPresence DMA system generates a packet capture file with the .pcap extension and prompts you to download the file.

6. Go to **Admin > System Log Files** and select the .pcap file to download.

7. Under **Actions**, click **Download Individual Logs** and select a location to save the file.
   - The system notifies you when the download is complete.

### Run Ping

Use **Ping** to verify that a RealPresence DMA system can communicate with another device in the network. You can run and see the results of the ping command on each server in a cluster.

#### To run ping on a system:

1. Go to **Admin > Troubleshooting Utilities > Ping**.
2. Enter an IP address or host name and click **Ping**.
   - The system displays the results of the command.

### Run Traceroute

Use **Traceroute** to see the route that the system uses to reach the address you specify and the latency (round trip) for each hop.

#### To run traceroute on a system:

1. Go to **Admin > Troubleshooting Utilities > Traceroute**.
2. Enter an IP address or host name and click **Trace**.
   - The system displays the results of the command.

### Run Top

Use **Top** to see an overview of your RealPresence DMA system’s current status, including CPU and memory usage, number of tasks, and list of running processes. The results automatically update every few seconds and you can see the updated results of the top command for the system.

#### To run top on a system

- Go to **Admin > Troubleshooting Utilities > Top**.
  - The system displays results of the command for each server.
Troubleshooting Utilities

Run I/O Stats

Run I/O Stats to see CPU resource allocation and read/write statistics for each RealPresence DMA system. For detailed information about the output of this utility, refer to the utility documentation at http://sebastien.godard.pagesperso-orange.fr/man_iostat.html.

To run I/O stats on a system:

» Go to Admin > Troubleshooting Utilities > I/O Stats.

The system displays the results of the command.

Run SAR

Use SAR to see a complete system activity report (from the preceding midnight to the current time) for each RealPresence DMA system.

To run SAR on a system:

» Go to Admin > Troubleshooting Utilities > SAR.

The system displays the results of the command.

Check NTP Status

Use NTP Status to see a list of clock sources known to each server (including the local clock) and their status. It runs the command ntpq -p on your RealPresence DMA system. For detailed information about the output of this utility, refer to the utility documentation at http://nlug.ml1.co.uk/2012/01/ntpq-p-output/831.

To check NTP status on a system:

» Go to Admin > Troubleshooting Utilities > NTP Status.

The system displays the results of the command.

Manually Synchronize all Clusters

The Manually Synchronize all Clusters feature synchronizes system configuration data across all servers in the supercluster and automatically repairs synchronization issues.

When you change configuration settings on a RealPresence DMA system, the changes are first stored locally on one of the systems in the supercluster, and synchronized soon after with the other systems. At times (usually during severe network outages), a server can lose data and the configuration becomes inconsistent between systems in the supercluster. Nightly, each individual DMA system automatically performs a self-check on its data and will fix inconsistencies if found. Manually synchronizing initiates this process immediately and simultaneously on all DMA systems (standalone or HA nodes) in the supercluster.
To manually synchronize all clusters:

1. Go to Admin > Troubleshooting Utilities > Manually Synchronize all Clusters.
2. Click OK to confirm the action.

Reset to Default Settings

A RealPresence DMA system can be reset back to its factory default configuration. A reset will clear most settings you have configured on the User, Integrations, and Service Config menus, and some settings on the Admin menu in the management user interface. A reset will also change the management user interface administrator password back to the factory default, but will not reset the system root password.

You cannot reset a system to the default settings if it is enabled for High Availability or is part of a supercluster. You must first disable High Availability or remove the system from the supercluster.

If you reset the system to its default configuration, the following settings will not be reset and will remain the same after your system reboots:

- Network settings
- Time settings
- Licenses
- Logging settings
- Security settings
- Certificates
- SNMP settings
- Alert settings
- Backup settings
- EULA acceptance

To reset to the default settings:

1. Go to Admin > Troubleshooting Utilities > Reset to Default Settings.
   The system displays a warning message.
2. Click OK to continue.
   The system displays a second warning message.
3. Click Yes to confirm.
   The system displays the login screen and then reboots with the default settings.
4. Log in with the factory-default credentials and reconfigure any changed settings as needed for your network environment.

Caution: This operation may take several minutes and may consume significant memory and CPU resources. Polycom does not recommend using this utility during peak traffic periods or while other resource-intensive tasks are underway (such as system backups, CDR downloads, or Microsoft Active Directory integration updates).
Diagnostics for your Polycom Server

You need to have a monitor and USB keyboard in order to run server diagnostics on your RealPresence DMA system, Appliance Edition hardware.

Perform these diagnostics only under the guidance of Polycom Global Services.